UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE CIENCIAS EMPRESARIALES

ESCUELA PROFESIONAL DE ADMINISTRACIÓN

Delitos informáticos y percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios, Chimbote - 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
LICENCIADA EN ADMINISTRACIÓN

AUTORAS:

Gonzales Ita, Mirtha Daniela (orcid.org/0000-0002-5117-089X)

Mantilla Barrón, Carmen Thalia (orcid.org/0000-0003-3022-4788)

ASESORES:

Dr. Espinoza de la Cruz, Manuel Antonio (orcid.org/0000-0001-6290-4484)

Dr. Salazar Llanos Juan Francisco (orcid.org/0000-0001-8314-2634)

LÍNEA DE INVESTIGACIÓN:

Gestión de Organizaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

CHIMBOTE – PERÚ

2022

Dedicatoria

Con gran afecto y amor se la dedico a mis padres, Martha Barrón y Agustín Mantilla, su ejemplo, apoyo y motivación son los detonantes de mi esfuerzo y ganas de superación. A mis hermanos porque juntos formamos un gran equipo, nos cuidamos, apoyamos mutuamente y nos sentimos orgullosos unos de otros. A Dios por darme la vida, salud y sabiduría en todo el proceso del desarrollo de ésta investigación. Llena de satisfacción, amor y esperanza, se las dedico a ustedes.

Carmen Thalia Mantilla Barrón

Esta tesis va dedicada principalmente a mis padres, Mirtha Ita Lombardi , Samuel Gonzales Luna y Luis Miguel Gonzales Ita, por su amor, trabajo y sacrificio durante todos estos años para lograr con éxito mi profesión, gracias a sus consejos, enseñanzas y valores , he llegado a lograr y concluir con éxito mis estudios y por ellos seguiré cumpliendo cada una de mis metas, a mis hermanos por ser parte de cada paso en mi vida, por la ayuda constante en mis proyectos y por enseñarme siempre a ser cada día mejor persona.

Mirtha Daniela Gonzales Ita

Agradecimiento

A Dios, quien me ama, guía y da la fortaleza para seguir adelante. Gracias papá, Agustín Mantilla, tu ejemplo de lucha y batalla ante la vida, es mi mayor motivación. Gracias mamá, Martha Barrón, por la confianza puesta en mí. Gracias hermanos por el apoyo incondicional. Agradezco a la Universidad César Vallejo, y sus docentes, especialmente al Dr. Manuel Antonio Espinoza de la Cruz por su apoyo y confianza en mi trabajo, además de su capacidad para guiar mis ideas ha sido un aporte invaluable en mi formación como profesional.

Carmen Thalia Mantilla Barrón

Gracias a mis padres por apoyarme en cada decisión y proyecto que he realizado a lo largo de mi vida, por ser fuente de inspiración, constancia y motivación sobretodo en el desarrollo de esta tesis. A nuestros maestros y compañeros por formar parte de nuestro camino como profesionales y ser base de valores, conocimiento y dedicación para alcanzar lo que nos proponemos.

Mirtha Gonzales Ita

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

El objetivo general de la presente investigación fue describir los niveles de percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote. Se trabajó con una investigación de tipo aplicada, diseño no experimental, de corte transversal de nivel descriptivo, en una muestra de 383 usuarios de la banca digital de entidades bancarias, así mismo el instrumento empleado para recolectar los datos fue el cuestionario y la técnica la encuesta. La validez del instrumento se hizo mediante el juicio de expertos y para la confiabilidad se utilizó el Alfa de Cronbach. Los resultados revelaron que la percepción de seguridad de los usuarios bancarios tiene un nivel medio (73.2%) con inclinación a bajo (21.1%), el nivel alto (5.7%) queda muy alejado de su percepción; esto puede darse por causas de fraudes y estafas que se avistan de forma recurrente en las transacciones en línea, y que hoy en día se les conoce como el cibercrimen. Asimismo, el nivel de fraude informática es bajo (81%), el de estafa informática está entre baja (50.3%) y media (48.4%), lo que permite atribuir que las estafas es el tipo de delito informático más recurrente en la banca en línea.

Palabras clave: delitos informáticos, percepción, seguridad, banca digital.

Abstract

The general objective of the present investigation was to describe the levels of perception of security of the clients in the online operations of the banking systems of Chimbote. We worked with an applied research, non-experimental design, cross-sectional descriptive level, in a sample of 383 users of digital banking of banking entities, likewise the instrument used to collect the data was the questionnaire and the technique the poll. The validity of the instrument was done through expert judgment and for reliability Cronbach's Alpha was used. The results revealed that the perception of security of bank users has a medium level (73.2%) with a tendency to low (21.1%), the high level (5.7%) is very far from their perception; This can be due to fraud and scams that are seen recurrently in online transactions, and that today are known as cybercrime. Likewise, the level of computer fraud is low (81%), that of computer fraud is between low (50.3%) and medium (48.4%), which allows us to attribute that fraud is the most recurrent type of computer crime in banking online.

Keywords: computer crimes, perception, security, digital banking.

I. INTRODUCCIÓN

En los últimos años, la tecnología y los sistemas informáticos con su notable desarrollo han generado cambios en las formas de operar de las empresas, es así que en la era de la automatización la prestación de servicios se ha ido digitalizando progresivamente. La respuesta del sector financiero a tal vertiginoso avance tecnológico está causando el replanteamiento de sus modelos de negocio de forma inminente, haciendo uso de la tecnología como propuesta a soluciones innovadoras para con sus usuarios, en la que no solamente ofrecen de forma tradicional sus servicios, sino que las mejoran.

El advenimiento de la tecnología financiera que permite al sector bancario beneficiarse y aprovechar al máximo este auge digital trajo consigo situaciones de riesgos por afrontar. Tal es el caso de los delitos informáticos que corresponden a fraudes y estafas mediante las tecnologías de información en la que suplantan la identidad de personas naturales y jurídicas. Entre sus efectos prevalece aquella que impacta de manera directa a la empresa, poniendo en juicio su imagen y percepción de seguridad que tienen sus clientes de ella. En relación, la Asociación de Bancos del Perú (Asbanc, 2020), dio a conocer que en el 2020 los fraudes realizados a las tarjetas más usadas en el país que son las de débito y crédito se dieron en un 38% por internet; cifra preocupante para los interesados.

Al margen de ello, en relación al entorno internacional, un reporte realizado por el Federal Bureau of Investigation (FBI, 2020, p. 13) conocido por sus siglas como el FBI, en su informe de delitos por internet, menciona que en Estados Unidos se ha registrado un crecimiento de denuncias presentadas por clientes de entidades financieras, generando más de 146 millones de dólares en pérdidas. La estafa es conocida como fraude de soporte técnico el cual consiste en engañar a sus víctimas haciéndose pasar por un personal de atención al cliente de instituciones financieras, ofreciéndoles resolver algún problema con su cuenta bancaria, para luego hacer transferencias bancarias a cuentas en el extranjero o comprar en grandes cantidades, siendo el 66% de las víctimas, adultos mayores de 60 años. Este problema no solo ocurre en Estados Unidos, en diversos países de América latina se ha registrado el mismo aumento, por lo que los gestores de riesgos corporativos buscan idear sistemas cada vez más óptimos que imposibilite a los delincuentes realizar sus hazañas.

Por otro lado, según la División de Investigación de Alta Tecnología (Diviant - Dirincri PNP, 2020), en el Perú los casos por delitos informáticos se han elevado en un 39.78%, solo en el año 2020 se investigaron un total de 4162 casos. Los principales fraudes denunciados en el Perú son las operaciones o transacciones con fondos no autorizados o nulos, otra modalidad es el phishing, que se basa en la creación de páginas falsas que simulan ser los sitios web de las entidades financieras para engañar y hacer que los usuarios se registren, procediendo al robo de sus datos personales y clonación de tarjetas (Pichigua, 2020).

En la ciudad de Chimbote, mediante una redacción de Ríos (2020) del Diario el Correo, destaca el preocupante incremento de los delitos informáticos a raíz de la emergencia sanitaria del COVID 19, en donde el departamento de investigación criminal de Chimbote registró hasta 50 denuncias por este tipo de modalidad delictiva en el 2020, para ello realizan distintos modus operandi como el envío de mensajes o llamadas telefónicas refiriéndose a bancos importantes de la ciudad para solicitar datos específicos de sus víctimas.

Esta disruptiva tecnológica que pone en riesgo el entorno electrónico de los bancos, ha proporcionado la necesidad de estudio en esta investigación basado en los aspectos relacionados a la seguridad percibida por los bancos y sus usuarios. Ante esta coyuntura, se adjudica el problema de investigación determinado en la interrogante ¿cuál es el nivel de delitos informáticos y la percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios, Chimbote periodo 2022?

En este sentido, este informe de investigación se justifica por su relevancia social, práctica y teórica tanto para las entidades involucradas como para la sociedad en general. Su contribución social se atribuye porque favorece a la comunidad financiera y sus consumidores bancarios al estudiar los movimientos digitales y la corresponsabilidad que existe entre los usuarios y el sector, analizando la sensibilidad de seguridad de ambas partes ante los riesgos delictivos eminentes si no se toman la seguridad del caso. En el aspecto práctico, se realiza un aporte investigativo donde las entidades financieras podrán recabar información actual y relevante sobre el fenómeno en cuestión, de tal forma que puedan actuar de manera coherente ante los insurgentes delitos y logren minimizarlos. Asimismo,

podrán analizar resultados en términos estadísticos relativos a la seguridad que se percibe en este contexto delictivo digital.

Finalmente, se considera que esta investigación es de relevancia teórica, al entenderse que los delitos informáticos es un fenómeno de reciente incidencia con impacto mundial que se ha ido acrecentando en todos los sectores del país, por lo que no hay suficientes investigaciones que se encarguen de su estudio y fundamenten su impacto a nivel social y empresarial como lo es el sector bancario peruano, en tal sentido, se estima que esta investigación amerite el interés por parte de futuros profesionales a que realicen investigaciones referentes de modo que se pueda seguir generando un aporte actualizado y de valor. Por conveniencia los investigadores asumen que los bancos líderes en Chimbote son Scotiabank, Interbank, BBVA y Continental por lo que se ajustará los cuestionarios a clientes de estas organizaciones bancarias

En el contexto de esta investigación, este fenómeno criminal denominado ciberdelincuencia que vulnera la confiabilidad e integridad de los sistemas informáticos hacen que exista una mayor percepción de inseguridad por parte de los usuarios bancarios.

En ese sentido, la presente investigación tiene como objetivo general describir los niveles de los delitos informáticos y la percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022. Los objetivos específicos son; describir las modalidades de delitos informáticos recurrentes a los que se ven expuestos los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote periodo 2022; describir el nivel de sensación de seguridad en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote periodo 2022; describir el nivel de seguridad informática en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote periodo 2022.

Además, se propuso un plan de contingencia en delitos informáticos para las operaciones realizadas en línea.

II. MARCO TEÓRICO

Las disquisiciones teóricas en esta investigación sobre los efectos de los eventos delictivos suscitado por sistemas informáticos, y la percepción de seguridad e inseguridad que recae sobre sus víctimas, tras el ámbito del daño en el desenvolvimiento de la actividad financiera, también podrá ser discutida; a modo que doctrinariamente se defiende la posición de responsabilidad que recae, por un lado, sobre el sistema bancario y por el otro, sobre los usuarios. En ambos casos, la perspectiva de las victimas va cambiar antes y después de haberse involucrado en un caso de fraude electrónico. Lo anterior se ha dicho para justificar el marco teórico que aquí será descrito.

Aunado a lo anteriormente expuesto, en el ámbito internacional, Angulo y Córdova (2019) con su investigación titulada “Análisis De La Taxonomía De Los Delitos Informáticos En El Sector Bancario Del Ecuador En El Período 2014 – 2019”, señala que tuvo como objetivo plantear un plan estratégico para ayudar en las medidas de precaución de los delitos informáticos en las entidades bancarias Ecuatorianas, realizó una investigación de campo de tipo descriptivo, en donde se encuestaron a un total de 60 personas, donde 50 fueron clientes del bancos, 8 expertos informáticos y 2 expertos en delitos informáticos. Los resultados demostraron que un 68% de los encuestados han sido afectados por robo de identidad. De este total, el 86% afirma que fue mediante páginas web. Asimismo, el 30% de ellos no obtuvo solución al problema. Concluyendo que es necesaria la puesta en marcha de procedimientos internos como proceso de: recuperación, de operación alterna y de restauración, además de capacitar permanentemente a clientes de bancos y a los administradores de justicia en temas de prevención y precaución de los delitos en las instituciones bancarias, puesto que él 70% de los encuestados considera que el banco del cual es cliente no es seguro en relación a este tipo de delitos.

Por su parte, Guerrero y Castillo (2017) con su tesis titulada “Desafíos Técnicos y Jurídicos Frente al Ciberdelito en el Sector Bancario Colombiano, Bogotá 2017”. Tuvo como objetivo de investigación analizar y comprender tanto el contexto como los tipos de ciberdelitos cometidos en el sector financiero, para generar tácticas que favorezcan a su prevención y tipificación en base a la legislación vigente de manera nacional como internacional. Su investigación fue de tipo descriptiva y su

diseño de investigación documental. No obstante, es plausible manifestar que este estudio es cualitativo en donde la fuente de compilación de información de datos secundarios estuvo enmarcada en investigaciones obtenidas de fuentes documentales como: Redalyc, Scielo, ESBCO, publicaciones de corporaciones oficiales y entidades bancarias de Colombia. Concluyendo que en Colombia las denuncias por ciberdelitos han aumentado en un 25% más respecto a los delitos por homicidios y narcotráficos. Por otro lado, un 75% de los ciberdelitos reportados son asociados al Sistema Financiero, destacando el phishing como el principal ataque, resaltando que estos delitos no se realizan por medio de aparatos tecnológicos sofisticados, sino que es ejecutado mediante correos electrónicos y aplicaciones móviles.

Por otro lado, Rodríguez (2020) en su tesis “Análisis de los delitos informáticos en base a la alteración y modificación mediante transferencia electrónica en modalidad tarjeta de crédito, Guayaquil 2020”, la misma tuvo por objetivo principal estudiar la correspondencia existente entre las formas de usurpación fraudulenta por canales electrónicos que son penados y la apropiación ilegal de datos, comprendidos en los artículos 230 y 190 del Código Orgánico Integral Penal y en base a ello formular componentes de prevención en las transferencias electrónicas mediante tarjetas de crédito. Se realizó una investigación cualitativa de tipología no experimental, la población estuvo constituida por 17258 profesionales en la rama de Derecho, con una muestra constituida por 376 abogados expertos en la rama de Delitos Informáticos y materia de Derecho Penal. El instrumento empleado fue la encuesta. Se obtuvo como resultado que un 40% testifica que la estafa más común específicamente mediante el uso de tarjeta de crédito es el fraude por causas de robo de identidad, de igual forma también un 40% de los abogados infiere que la frecuencia con la que se realizan estos actos es muy alta. En relación a las causas, un 60% argumenta que se produce por errores propios de los usuarios, al facilitar información personal por medio del correo electrónico, herramienta principal utilizada por delincuentes para cometer tal calamidad. Finalmente, concluyó que resulta irrelevante hacer primero un estudio global sobre ciberdelitos en los bancos para luego realizar su análisis a nivel nacional, el 70% de los profesionales encuestados está de acuerdo con esta propuesta. Además, se orienta a poner énfasis en las modalidades más usadas

en estos delitos, en la que el 50% considera que hacen uso de llaves que facilita el libre acceso a los archivos de ordenadores aun sin tener previa autorización.

En el entorno nacional, Cardich, (2020) con su tesis titulada “La Auditoría Forense y Su Incidencia en la Gestión de Riesgo de Fraude de las Cajas Municipales de Ahorro y Crédito en el Perú, 2016-2017”, tuvo como objetivo el indagar sobre las formas de prevenir, detectar y otorgar solución a los riesgos por fraude y de qué manera la auditoría forense ayuda a corregir la gestión de riesgos de los programas de detección y prevención de pérdidas económicas que se generan con las conductas delictivas. Por lo cual se realizó una investigación descriptiva, en donde se encuestaron a 80 profesionales pertenecientes al área de Gerencia de Auditoría Interna (GAI), al área de Riesgo Operacional-RO y el área de Órgano de Control Institucional (OCI). Los instrumentos empleados fueron la encuesta a clientes del sistema bancario y entrevistas a expertos informáticos de bancos y expertos en delitos informáticos. Dando como resultado que un 58.8% afirma estar de acuerdo en que la auditoria forense contribuye en gran medida a vigorizar el sistema interno de control Interno de las financieras de ahorro y crédito en cuestión de prevención y detección de fraude. Por otro lado, un 45% de los profesionales sostienen que las Cajas Municipales de Ahorro y Crédito incorporaron de manera óptima y adecuada la gestión de riesgo en el ámbito del fraude; mientras un 23,8% se contrapone en total desacuerdo. En conclusión, en base a los datos estadísticos alcanzados se refleja la percepción de los clientes respecto a los delitos informáticos los cuales se muestran en estado de indefensión. Para tal caso, se identificó la necesidad de implementar un modelo que ayude en la mitigación de delitos cibernéticos críticos, para lo cual es necesario realizar capacitaciones respecto a su prevención y detección.

Asimismo, Córdova y Barios (2018) en su investigación titulada “Análisis de los principales factores financieros, operacionales y de reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú como son Banco de crédito del Perú y Banco Continental en los últimos 5 años” tuvieron como propósito analizar cómo impacta de manera operacional, financiera y de imagen corporativa el aumento de los delitos informáticos en dos bancos importantes de Lima Metropolitana como son el Banco de Crédito del Perú y BBVA en los últimos 5 años. Realizó una

investigación cualitativa, descriptiva; entrevistó a 23 personas que constaron de 13 clientes y 10 trabajadores de las respectivas entidades. El instrumento de investigación utilizado fue el cuestionario. En torno a los resultados se identificó que por día se realizan entre 12 a 20 reclamos por fraudes, lo que corresponde a un aumento del 600% ya que años atrás se suscitaban 2 reclamos diariamente como máximo. En consecuencia, el número de trabajadores analistas de fraude en los bancos también se han duplicado de 2 a 4 colaboradores. En conclusión, se argumentó que, las entidades financieras han ido optimizando y cambiando sus estrategias operativas para desempeñarse en el cumplimiento de prevención, localización y monitoreo de estos fraudes, implementando dispositivos de seguridad, como el caso de BCP con el "Token" incorporado a sus plataformas, puesto que, a nivel nacional se reportaron hasta 16 millones de transacciones bancarias correspondiéndole a la entidad financiera el 50% de ellas. Por otro lado, resaltan que debido a que se ha visto afectada su reputación, estas están en constante capacitación y adquisición de nueva tecnología que contribuya a minimizar los riesgos de delitos. Por último, destacan que el impacto financiero se refleja por la fuerte inversión en infraestructura y aplicaciones tecnológicas que permitan proteger adecuadamente a la entidad y a sus clientes, mencionando que hace 4 años ponían a disposición el 2% de su presupuesto económico en seguridad, mientras que actualmente se adjudica el 8%.

Por su parte, Zambrano (2021) con su tesis titulada "El uso de Banca Móvil en los Delitos Informáticos contra el patrimonio en la ciudad de Arequipa, 2020". Tuvo como objetivo establecer si la utilización y manejo de la banca móvil incentiva el aumento de delitos informáticos en la ciudad de Arequipa, por lo cual se realizó una investigación básica – cualitativa, realizando una entrevista estructurada a una muestra conformada por 10 especialistas de investigación de delitos de alta tecnología, fiscales penales, abogados y peritos en materia de delitos informáticos. Obteniendo como resultado que un 50% de los entrevistados afirman que la banca Móvil si promueve el fraude y delitos informáticos, debido a su uso masificado ha sido blanco para los ciber delincuentes, además de que también promueve la clonación de datos ya que para acceder a ella es necesario contar con datos como número de cuenta, número de tarjeta, código de seguridad y fecha de vencimiento de la tarjeta.

El marco teórico conceptual sobre la variable delitos informáticos en el sistema financiero surge a partir de las teorías de diferentes autores.

En relación, Temperini (2018, p. 54) citando a Leiva, infiere que el delito informático corresponde a cualquier acción típica, ilícita y culpable, en donde el medio para ejecutarla es la tecnología a través del ordenador. De manera similar, Ávalos (2021, p.12) manifiesta que el delito informático, en un sentido estricto, engloba cualquier comportamiento ilegal que sitúe en peligro la seguridad de los sistemas informáticos y el procesamiento de datos a través de operaciones electrónicas. Además, Temperini, (2018, p. 54) citando a García, menciona que los delitos informáticos deberían ser vistos desde tres puntos de vista: como fin, donde la computadora sea objeto para dañar o manipular la información que contenga, como medio, usando el ordenador como herramienta para facilitar el delito y por último como objeto de prueba, guardando pruebas incidentales de los delitos ejecutados en la computadora.

En la perspectiva de Ospina y Sanabria (2020) lo definen como actos que ponen en peligro o dañan la integridad, confidencialidad, privacidad o los recursos disponibles de datos y procedimientos informáticos, por medio de aparatos tecnológicos, aplicaciones móviles, transacciones electrónicas, etc., vulnerando a personas, empresas y gobiernos. En concordancia, Temperini (2018, p. 53) infiere que la tecnología es una especie de potenciador de este tipo de delitos, pues el crimen no es nuevo, sino que al combinarse con ciertas características de las nuevas tecnologías terminan llevando al delito a un nuevo nivel.

En conclusión, teniendo en cuenta las definiciones de los autores anteriormente mencionados, se puede inferir que los delitos informáticos se basan en conductas ilícitas realizadas por medio de aparatos electrónicos con el objetivo de dañar u obtener de manera ilegal información y datos personales, afectando la seguridad y patrimonio del sujeto, empresa o gobierno que resulta víctima. En la era de la digitalización de las cosas los ciberdelitos se han ido acrecentando aun cuando, como dice Bokovnya (2020), la educación de las personas respecto a la digitalización es cada vez mejor.

En relación a las peculiaridades de los delitos informáticos, Temperini (2018, p.61) citando a Téllez menciona que los sujetos que ejecutan esta modalidad de delitos tienen la habilidad y conocimientos para manejar los sistemas informáticos y las

características que presentan son: conductas que sólo una cantidad determinada de sujetos con conocimientos técnicos específicos pueden realizarlo, mayormente son comportamientos generados por el victimario cuando el sujeto que es víctima está laborando, son actos oportunos porque se aprovecha el momento creado con intención o no, en las funciones que tienen relación al sistema tecnológico y económico, provocan alarmantes pérdidas económicas, son muy fáciles de llevarse a cabo según espacio y tiempo, ya que pueden consumarse en menos de un segundo y sin necesidad de estar presente físicamente, se registran muchos casos pero escasas denuncias porque no existe una clara regulación jurídica de entorno internacional y por el miedo a la denigración de imagen de la organización afectada, suelen ser muy difíciles de comprobar, por su carácter técnico, mayormente son delitos intencionales y tienden a incrementarse de manera ascendente, por lo que se necesita de manera inaplazable una regulación jurídica en el ámbito internacional.

Téllez (2008) citando el Manual de las Naciones Unidas a fin de contribuir a la mitigación y el control de los robos informáticos señala los tipos de delitos informáticos más resaltantes; el primero corresponde a fraudes ocasionados a través del manejo de computadoras, estas a su vez tienen tres características; una de ellas es la manipulación de datos entrantes que constituye el delito informático más habitual, por ser el más factible de realizarse, pero difícil de resultar descubierto, no necesita de habilidades en informática, consiste en la sustracción de datos por una persona que tenga acceso a información, la otra corresponde a la manipulación de programas que es un método utilizado por personas con conocimientos en programación, denominado Caballo de Troya, en donde se insertan instrucciones encubiertas en los programas informáticos para realizar funciones no autorizadas por el propietario al mismo tiempo de que se ejecuta y realiza su trabajo de manera normal, luego está la manipulación de los datos salientes que son utilizados en aparatos y programas expertos en recopilar la información electrónica adulterada en las bandas magnéticas que se disponen en las tarjetas bancarias. y por último el fraude perpetrado por manejo informático que se favorece de las repeticiones automáticas de los procesos informáticos, en donde se transaccionan pequeñas cantidades de manera repetitiva de una cuenta a otra.

El segundo tipo de delito pertenece a las adulteraciones informáticas; estas pueden realizarse como objeto cuando causa la alteración de datos recopilados digitalmente o como instrumentos que significa la falsificación o alteración fraudulenta de documentos de uso comercial, mediante equipos computarizados y fotocopiadoras a base de rayos láser. El tercer tipo de delito son los perjuicios o modificación de programas computarizados, estos pueden ser por sabotaje informático que consiste en eliminar o modificar sin autorización de su propietario información o funciones de su computador para que este no funcione de manera correcta; por virus que son una serie de códigos de programación que se adhieren a los programas informáticos que son genuinos de la computadora y propagarse hacia otros; por gusanos que son similares a los virus solo que en este no hay propagación hacia otros programas, pero las consecuencias son igual de graves debido a que mediante ellos los delincuentes pueden facilitar instrucciones a un sistema informático de una entidad a transferir dinero de manera ilegal y por bomba lógica o cronológica que es un programa que trabaja cronológicamente para alterar información o datos a futuro. El cuarto tipo de delito informático son las falsificaciones informáticas que se dan por piratas informáticos o hackers; y consiste en que los hackers se hacen pasar por clientes del sistema para obtener contraseñas e información que esta accesible en la red de telecomunicaciones; otra forma es la reproducción no autorizada de programas informáticos de protección legal; que genera muchas pérdidas económicas a sus propietarios por lo mismo están sometidas a sanciones penales.

No obstante, resulta imprescindible conocer a qué se refiere fraude, estafa y hurto informático para identificar su diferencia. De acuerdo a fraude informático Mayer y Oliver (2020) mencionan que son acciones que provocan daños patrimoniales mediante la manipulación o modificación de datos o programas del sistema informático. Aquello puede ocurrir de dos formas, la primera de ellas es por medio de fraude al sistema, acto que Pardo (2018) señala que es el fraude donde el sujeto que comete el delito burla las medidas de seguridad de los medios o sistemas informáticos utilizando su experiencia y conocimientos en informática para acceder al patrimonio virtual de la víctima; y la segunda es por fraude en los datos, en la que el mismo autor, alude que es aquel que se caracteriza por alterar

los datos en los sistemas informáticos a fin de conseguir beneficios económicos (pp. 61-62).

En relación a estafa informática Pardo (2018) menciona que es un acto delictivo, que incluye el uso de computadoras para engañar a las víctimas para que se deshagan de su patrimonio y al uso indebido del patrimonio por parte de los delincuentes (p. 62). Las estafas más recurrentes según el BCP son el phishing que es una modalidad de estafa que consiste en el uso de correos electrónicos que tienen la apariencia de pertenecer a fuentes de confianza para sacar información personal de clientes de bancos y sus cuentas bancarias de forma fraudulenta (Villón, et al., 2019, p. 673). Una de las formas de estafar bajo esta modalidad es, como nos dice Hossein (2021), cuando los usuarios honestos son engañados con sitios web de pishing, creyendo que están interactuando con páginas web legítimas. El 91% de los ataques digitales empiezan con un correo electrónico de pishing (O'Leary, 2019). Otra de las estafas más comunes es el Smishing; Elif y Bagriyanik (2020) mencionan que es una modalidad de estafa realizada a través de mensajes de texto o SMS, haciendo uso de URL abreviado y con alias como por ejemplo Bitly, en donde se hacen pasar por fuentes confiables de bancos para engañar y obtener información personal. Y el Vishing; modalidad donde los atacantes usan llamadas telefónicas anónimas o promociones falsas para engañar a los usuarios para que revelen sus PIN u otra información personal confidencial que se usa para robar sus cuentas de dinero móvil (Ali, Mussa, & Sam, 2020, p. 5). Una de las maneras de evitar ser engañado bajo estas modalidades es la capacitación; Jensen (2017) en un trabajo de investigación en Estados Unidos bajo un estudio de campo comprobó que las personas que tuvieron capacitación respecto a los ataques de pishing pudieron detectar y evitar de una mejor forma los ataques en relación con los que no habían sido capacitados; concluyendo que el entrenamiento antipishing es una gran vía de evitamiento de ciberdelitos.

Y, por último, hurto informático según la perspectiva de Domenech y Ortiz (2015, como se citó en Pardo, 2018, p. 58) menciona que es la apropiación ilícita de software o información, en donde el sujeto accede a un computador ajeno, vulnerando o alterando archivos informáticos para apoderarse del patrimonio de terceros y guardarlos en un soporte propio. Puede darse como hurto sistemático;

que se basa en el robo continuo del patrimonio de una persona por medio de sistemas informáticos (como cuentas bancarias). Donde los delincuentes retiran de manera regular y continua los ahorros o montos en la cuenta, transfiriéndolas a otras o realizando compras; o hurto de valores en la que no solo el dinero puede ser objeto de sustracción informática, sino que también hay otros bienes de relevancia patrimonial como los valores digitales, se refiere al hurto de bienes como títulos de valores, programas, y otros (Pardo, 2018, p.59).

Por lo tanto, la diferencia consiste en que fraude informático hace alusión a la alteración de datos que evoca la generación de un perjuicio patrimonial, a diferencia de estafa informática que se refiere a un engaño que se puede perpetrar por medio de la comunicación telefónica o por un ordenador por ejemplo en el envío de mensajes o correos. Hasta aquí la diferencia está en el medio, en la que fraude es la alteración de datos y estafa el engaño o error. Y, por último, el hurto sistemático da cuenta de suplantación de identidad o su usurpación, es decir tiene que ver con la apropiación.

En congruencia, al igual que las tecnologías, los delitos informáticos han abarcado todos los ámbitos sociales. De acuerdo a su impacto en el ámbito mundial, Aguilar (2020) mencionó mediante su artículo sobre delitos informáticos en la página de Business Insider que la compañía mundial de ciberseguridad y servicios de antivirus McAfee manifestó mediante un comunicado que los delitos informáticos han ocasionado pérdidas monetarias superiores al 1% del PBI mundial, esto quiere decir más de un billón de dólares, argumentando que los daños no solo son financieros sino también afectan el rendimiento de los negocios ya que los ciber delincuentes encriptan sus activos digitales hasta que las compañías paguen un rescate, lo que genera gran pérdida de tiempo y dinero. La compañía realizó un informe a nivel global donde encuestó a 1500 profesionales responsables de firmas en ciberseguridad de Estados unidos, Reino Unido, Francia, Japón, Canadá y Australia quienes cuentan con más de 1000 empleados, un 33% de los encuestados revela que estos periodos de inactividad generan pérdidas de 100,000 a 500,000 dólares. Además de que a esto se suma la fuerte inversión que realizan los negocios en ciberseguridad para prevenir estos ataques, puesto que un 56% de las entidades encuestadas no cuentan con un plan para prevenir delitos informáticos, mientras que del 44% afirmó tener un plan,

un 32% aseguraba que si resultaría efectivo en caso de que ocurriera un ciberataque.

Su impacto en el ámbito internacional, la Agencia Internacional de Noticias EFE (2021) afirma que en Latinoamérica los delitos informáticos han aumentado en un 24% en el año 2020; tal como lo afirma Sánchez, et, al. (2017), en la actual era digital el internet de las cosas se encuentra involucrado en todos los campos. Es así que mediante una prensa virtual por la compañía internacional de seguridad informática Kaspersky infirió mediante los datos obtenidos por sus usuarios que el aumento se da por el auge del teletrabajo a causa del COVID 19, en donde prevalece Ecuador con un incremento de 75%, Perú con 71%, Panamá con 60%, Guatemala con 43% y Venezuela con 29%. Por otro lado, Brasil genera 1390 infecciones de malware por minuto, México una cantidad de 299 infecciones por minuto, Perú 96 infecciones por minuto, Ecuador 89 infecciones por minuto y Colombia 87 infecciones por minuto. En cuanto a la modalidad de delitos informáticos, afirma Kaspersky que Brasil figura en el primer ligar con 15,37% por intentos de ataques cibernéticos, Ecuador con 13,36%, Panamá con 12,60% Chile con 11,90% y Colombia con 11,09% de ciberataque mediante programas piratas donde obtienen control total de los dispositivos, archivos PDF para robar datos de tarjetas de crédito e información personal y anuncios maliciosos mediante coreos electrónicos. Finalmente puntualizo el riesgo de ataque que existe mediante la modalidad de ataque "la mano fantasma", en donde el delincuente entra al dispositivo mediante engaños por links o páginas web falsas en donde la victima ingresa con un solo clic y descarga, sin saberlo, un archivo malicioso que le permite acceder de manera remota a sus dispositivos, permitiéndole abrir aplicaciones bancarias y hacer transacciones, incluso cuando el aparato está apagado. Si bien el avance de la tecnología tiene relación directa con el incremento de ciberdelitos, una de las grandes causas en países como Ucrania es según Najar y Alemán (2017) la baja educación de la población en tecnología e información.

Finalmente, su impacto a nivel nacional, Ávalos (2021, p. 20) menciona, siguiendo la información contenida por parte de la División de Investigación de Delitos de Alta Tecnología de la Policía nacional del Perú (DIVINDAT), que desde el periodo 2013 a finales del año 2020, se han registrado 12,169 delitos, en donde el 78%

que corresponde a 9,515 registros, un 13% pertenece a suplantación de identidad y un 6% a delitos contra datos y sistemas informáticos. Infiriendo que el delito con mayor cantidad de registro de delitos informáticos corresponde a operaciones y transferencias electrónicas o fondos no autorizados, con un 86% que corresponde a 8,142. Además, Pichihua (2021) mediante la página de noticias Andina, informó que en el 2020 la DIVIDAT mencionó que las denuncias por delitos informáticos se han elevado a un 39,78%, registrándose más de 300 casos cada mes, donde el 84% de denuncias recibidas son por este tipo de delitos, resaltando el phishing como modalidad principalmente usada por los ciber delincuentes para engañar a los usuarios mediante paginas falsas que simulan ser las páginas web de los bancos y entidades financieras.

El impacto de los delitos informáticos particularmente en las entidades bancarias del Perú, tal como lo menciona Vargas (2019), cada año los bancos y financieras peruanas reciben un total de 180,000 quejas de sus usuarios referente a disconformidad en la atención, entre enero y junio del año 2019, Indecopi registró 12,941 reclamos contra bancos y financieras, convirtiéndose el sector bancario en uno de los más denunciados históricamente. En donde el Banco de Crédito del Perú lidera con 15.5% del total , seguido de Interbank con un 11.29% , Scotiabank con 9.2% y Banco BBVA con un 8.41%, destacando la modalidad de fraude según los principales bancos el phishing que consiste en el apropio de información a través de correos electrónicos falsos con el link de la página web con el motivo de actualización de datos, por otro lado se encuentra el Smishing, que son los SMS falsos en donde solicitan actualización de datos de tarjetas o cuentas, por último el Vishing que son fraudes por medio de llamadas telefónicas donde solicitan datos confidenciales del usuario.

Siguiendo con el marco teórico de las variables de estudio de esta investigación, las teorías relacionadas a la variable dependiente percepción de seguridad empieza con Sánchez (2018) quien la define como todo aquello que mide la sensación de la persona en relación a situaciones de seguridad o inseguridad en el medio donde se desenvuelve, desde el ángulo emocional en donde intervienen el miedo, rabia, ansiedad, etc., así como desde el punto institucional en base al desconocimiento, desconfianza e incertidumbre, por lo tanto, esta percepción

afecta de manera positiva o negativa a la calidad de vida y comportamiento de la persona.

En relación a la percepción de seguridad que tienen los sujetos víctimas de fraude financiero, el portal de noticias y revista para emprendedores Gana Más (2019) mencionó en su artículo, sobre la conferencia organizada por Emprende UP, en donde el socio de CMS Colombia Lorenzo Villegas, comentó que, en la región 9 de cada 10 entidades bancarias, que corresponde al 90%, son el blanco principal de los ciber delincuentes, siendo el sector más atacado en el último año, donde el 37% si llegaron a ser víctimas de robo. Por otro lado, afirma que el 39% de los incidentes por delitos informáticos no son reportados, variando la cifra en base al tamaño de la entidad financiera, llegando a 19% en entidades más grandes. Por último, destaca la percepción de seguridad adoptada por los usuarios, ya que 6 de cada 10, lo cual corresponde a un 60% no usa la banca digital porque desconfía de la seguridad en las transacciones efectuadas.

En concordancia, la página de noticias Verified News Explorer Network (2021) mediante un estudio de la empresa IPSOS menciona que, en Chile, la percepción de inseguridad de los clientes de instituciones financieras es muy alta puesto que 3 de cada 4 usuarios de bancos que corresponde al 75% han recibido correos o mensajes de texto considerados una amenaza de fraude cibernético y llamadas telefónicas con intención de robo de información. además de que 1 de cada 4 clientes ha sido víctima de fraude por clonación o uso fraudulento de medio de pago por tarjeta de crédito o débito, donde más del 25% ha vivido esta situación más de una vez. Por otro lado, menciona que el 95% de los afectados ha denunciado el fraude a su entidad financiera pero solo el 56% pudo recibir de regreso su dinero, mientras que el 31% no obtuvo solución, contestación y mucho menos indemnización por parte de la entidad financiera. Por último 2 de cada 3 personas lo cual corresponde el 67% creen que las instituciones no están invirtiendo en seguridad para proteger las transacciones e información de sus usuarios. En palabras de Jacome & Villamizar (2019) las empresas deberían realizar una elección minuciosa de software competentes que permitan realizar una buena gestión de seguridad en las operaciones en línea.

La empresa de telecomunicaciones Optical Networks (2018) mencionó que, en Perú, diariamente se registran cientos de delitos informáticos a entidades del

sector financiero asegurando que esta vulnerabilidad está asociada a la poca inversión que hacen las entidades financieras para prevenir y hacer frente a los delitos informáticos, del 100% del presupuesto que utilizan los bancos para invertir, solo el 15% es para ciberseguridad quedando expuestos a los ciber delincuentes. Aconsejándoles invertir al menos un 25% en ciberseguridad a fin de prevenir cualquier ataque y mantener a sus usuarios más seguros. Aunque, como lo manifiesta Santisteban et al. (2020), se gastan millones de dólares en todo el mundo para prevenir los ciberataques, pero a menos que las organizaciones trabajen de manera integral, estas amenazas seguirán perturbando las operaciones de las entidades.

Resulta imprescindible tener en cuenta los niveles de seguridad existentes en el ámbito de la seguridad informática; que en palabras de Vieites (2006, como se citó en Ausecha, et al. 2021) se refiere a cualquier medida usada para prevenir la ejecución de operaciones no permitidas sobre un sistema o red, cuyo impacto puede causar daño a la información, comprometer la confidencialidad, integridad, o reducir el rendimiento del equipo a fin de evitar que los usuarios autorizados accedan al sistema.

Entre los niveles de seguridad se identifican tres: peligroso, dudoso y seguro. Cuando la seguridad pertenece a un nivel seguro hace alusión a la condición de ciertos mecanismos que aseguran estar libre de todo daño, amenaza peligro o riesgo, esto quiere decir que la seguridad es, tal como lo refiere Mori (2019), componentes que favorecen un funcionamiento óptimo de algo.

En cuanto a las sensaciones de seguridad implica la percepción de confianza, incertidumbre y amenaza del sujeto usuario de la entidad financiera. En la línea de la confianza, Alburqueque (2018) menciona que es la esperanza o seguridad que tiene un individuo en alguien o en algo.

La incertidumbre es una situación de desconocimiento o imposibilidad de medir o calcular los sucesos que ocasionan daños. En ese sentido, la incertidumbre del nuevo consumidor tecnológico de hoy, tiene que ver con las formas de compra-venta totalmente digital a la que se enfrentan (Chavarro, 2018, p. 66).

A propósito de gestión de riesgos sistemáticos, es una dimensión que amerita tres análisis en relación a la percepción de riesgos de los usuarios bancarios; la primera de ellas es la prevención de riesgos que son un conjunto de acciones que

realiza la organización a fin de minimizar cualquier evento futuro que pueda causar daños tantos físicos como de seguridad para sus clientes y trabajadores. (Boletín Oficial del Estado, 2017, p.3). La segunda las políticas adoptadas; que refiere a pautas para marcar los límites a los que deben producirse las acciones. Las políticas son decisiones eventuales que pueden reducir conflictos en la definición de objetivos (Chiavenato, 2017, p.38); y la tercera los aspectos normativos; en palabras de Corti (2016) son un conjunto de normas o reglas aplicadas a una determinada actividad o asunto con el fin de establecer su funcionamiento (p. 156).

En concordancia, dada la preocupación por proteger la seguridad de las personas ante delitos informáticos, en América Latina, se ha incorporado en los últimos tiempos el Habeas Datas, este recurso constitucional es una garantía que protege los derechos de información y protección de datos privados, lo que involucra desde lo personal hasta lo financiero. Al mismo tiempo cada país ha decidido crear leyes de protección de sus ciudadanos, si su información personal se utiliza de una forma indebida (Parraguez & Caldera, 2016).

Desde otra perspectiva, Allasani (2017) sostiene que con el arribo del Word Wide Web (WWW) la banca electrónica y todo el comercio electrónico se han visto envueltos en concomitantes riesgos, dando pie a las organizaciones la gestión de las actividades de sus colaboradores por medio de políticas de seguridad de tecnología e información, especificando lo que se hace y no se hace en la utilización de sistemas informáticos. Además, las organizaciones tienen que actualizar constantemente las formas de prevención, así como avanza la tecnología, los riesgos cambian, se vuelven más consistentes y se adaptan a lo tecnológico, por tanto, Mugarza, Flores & Montero (2020) consideran que es necesario que las empresas realicen un seguimiento a las vulnerabilidades y amenazas detectadas para aplicar las medidas adecuadas como medio de garantía a la ciberseguridad.

Con el aumento del teletrabajo donde las actividades de las organizaciones se desplazaron hacia los hogares, la ciberseguridad no tiene el mismo nivel que en las empresas; esto podría considerarse una de las causas por la que se ha disparado el número de ataques, aprovechándose de las vulnerabilidades de los equipos u ordenadores domésticos (Andrade, Ortiz & Cazares, 2020).

Esta investigación y todos sus aportes tienen su base en las teorías de la administración científica, cada una de ellas han surgido en periodos de tiempos diferentes, sin embargo, ninguna es excluyente; ya que la que precede se encarga de levantar los aportes que se dieron con anterioridad.

La teoría de la contingencia como parte de las teorías de la administración permite cambiar el modo de ver a la organización, es decir, verlas desde adentro hacia afuera. Esto quiere decir que deben ajustarse de manera sistemática al entorno cambiante del ambiente, ese cambio organizacional es lo que se denomina contingente porque nada es absoluto, sino que siempre depende de algo en la teoría de la administración. Dentro del ambiente general se encuentran las condiciones tecnológicas que se relacionan con esta investigación y se refiere al desarrollo tecnológico que se da en el ambiente y afecta a la organización.

Este modelo de teoría de la contingencia fue propuesto por Víctor Vroom, que sustituye a las teorías de Maslow, McGregor y Herzberg (Chiavenato, 2019, p. 322). Cuando a tecnologías se refiere, la era actual que corresponde a la Revolución 4.0 tiene como una de sus características la digitalización de las operaciones empresariales (Chiavenato, 2019, p. 370), y los efectos que ellas generan como el caso de los delitos informáticos, modelo de estudio de esta investigación.

A este ritmo de crecimiento de la innovación se le denomina la “quinta ola”, denominado así por Schumpeter en 1990, quien argumenta que una economía sustentable es la que aniquila el equilibrio a través de la innovación tecnológica (Chiavenato, 2019, p. 495). Es así que el internet de las cosas en la actualidad es totalmente inevitable y es considerado por Hassani, et. al, (2021) la columna vertebral de la industria 4.0.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1 Tipo de investigación

Según el propósito, la investigación fue de tipo aplicada. Este tipo de investigación está dirigida a solucionar problemas que se presenten en el consumo de bienes y servicios, así como sus procesos de producción y distribución. Se les llama aplicada porque en relación a la investigación básica en las ciencias formales se crean problemas de trabajo o hipótesis para dar solución a problemas de la vida productiva de la sociedad (Nicomedes, 2018).

En relación, Cabezas, et al. (2018, p. 34) argumentan que el tipo de investigación aplicada tiene como fin principal buscar información empírica sobre aquellos problemas que se dan dentro del entorno institucional con el propósito de obtener opciones de solución. Por tanto, esta investigación estuvo orientada a lograr un conocimiento nuevo que posibilite solucionar problemas prácticos (Álvarez, 2021).

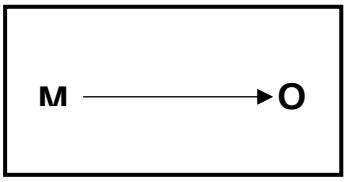
Según el nivel, la investigación a aplicar fue descriptiva. En referencia a la investigación descriptiva, Cabezas, et al. (2018) estipulan que se encarga de medir y recolectar datos de diferentes conceptos relacionados al fenómeno de investigación. La información reunida tuvo su origen en diversos autores respecto a las dos variables de investigación, así como a sus dimensiones e indicadores (p. 68).

3.1.2 Diseño de investigación

Por otro lado, la investigación contará con un diseño no experimental de corte transversal, debido a que se hará una investigación de campo, en un determinado periodo de tiempo, recolectando datos directamente de los usuarios de bancos sin cambiar las variables estudiadas. De acuerdo a ello, Cabezas, et al., (2018) sustentan que el estudio de índole no experimental sucede cuando no se manipula de manera intencionada las variables o conceptos. Su propósito de la investigación no experimental es indagar mediante la observación los fenómenos que ocurren en el medio natural y luego analizarlos (p. 79).

Como se puede observar en la figura 1, representa el diagrama de la investigación descriptiva que se realizará en este proyecto.

Diseño de investigación



Donde:

M: representa la muestra en que se realizará el estudio

O: es la observación de la muestra

3.2. Variables y Operacionalización

Las variables de este proyecto de investigación conformado por percepción de seguridad y delitos informáticos, tienen las siguientes definiciones:

Variable 1: Delitos Informáticos

Ospina y Sanabria (2020, p.200) lo definen como actos que ponen en peligro o dañan la integridad, confidencialidad y disposición de información y sistemas informáticos, por medio de aparatos tecnológicos, aplicaciones móviles, transacciones electrónicas, etc., vulnerando a personas, empresas y gobiernos.

Variable 2: Percepción de Seguridad

Según Sánchez (2018, p.1) como todo aquello que mide la sensación de la persona en relación a situaciones de seguridad o inseguridad en el medio donde se desenvuelve, desde el ángulo emocional en donde intervienen el miedo, rabia, ansiedad, etc., así como desde el punto institucional en base al desconocimiento, desconfianza e incertidumbre, por lo tanto, esta percepción afecta de manera positiva o negativa a la calidad de vida y comportamiento de la persona.

Definición Operacional:

La variable de estudio reconocida como independiente (Delitos informáticos) será medida a través de las dimensiones fraude informático, estafa informática y hurto informático. Su escala de medición será de tipo ordinal. Respecto a la variable dependiente (percepción de seguridad) será medida mediante las dimensiones Niveles de seguridad, Sensaciones de seguridad, Gestión de riesgos sistemáticos. Asimismo, su escala de medición será de tipo ordinal. Estas variables están conceptualizadas en el anexo 1, el cuadro de matriz de operacionalización de variables.

3.3. Población, muestra, muestreo, unidad de análisis

3.3.1 Población

Según Ventura (2017) menciona que una población es un grupo de personas, objetos o acontecimientos con características comunes cuyas propiedades se analizarán. En este informe de investigación la población estudiada la conformaron los ciudadanos de los distritos de Chimbote y Nuevo Chimbote, con una población total de 214,198 según el Instituto Nacional de Estadística (INEI, 2017).

Criterios de inclusión

- Personas femeninas y masculinas de 18 a 60 años de edad.
- Personas residentes de Chimbote y Nuevo Chimbote.
- Clientes de entidades bancarias: BCP, Interbank, Scotiabank y BBVA.

Criterios de exclusión

- Sujetos menores de edad como niños ya que no es posible considerarlos usuarios de entidades bancarias. Asimismo, mayores de 60 años que por su avanzada edad generalmente otorgan el poder de sus trámites bancarios a un tercero de confianza.

3.3.2 Muestra

Respecto a la muestra Díaz (2016) la define como la extracción de una porción representativa de la población ya definida o delimitada sobre la cual se recolectarán datos. Para seleccionar la muestra es necesario tener delimitado estas características de la población.

Teniendo en cuenta la necesidad de recopilar información específica del tema de estudio se eligió a 383 personas que cuentan con las características de ser usuarios de los bancos a investigar, el cálculo se determinó teniendo en cuenta una formula estadística finita que se encuentra detallada en anexos.

3.3.3 Muestreo

La investigación utilizó la técnica de muestreo no probabilístico y el método por conveniencia. Cabezas, et al. (2018, p.100) mencionan que el muestreo no probabilístico se refiere a la selección de un conjunto de elementos para la muestra, siendo utilizadas en investigaciones que requieren una selección de muestra con determinadas características. Y en el método por conveniencia las unidades de estudio se seleccionan al momento de la recolección de datos. Sus

características destacadas es que es accesible, factible, y económico, pero posee poca representatividad.

Unidad de análisis:

Para obtener los resultados del trabajo de investigación se tuvo en cuenta la muestra de investigación la cual consta de personas que residen en los distritos de Chimbote y Nuevo Chimbote, con un rango de edades entre 18 a 60 años, del sexo femenino y masculino, que son usuarios de entidades bancarias.

3.4. Técnicas e instrumentos de recolección de datos

Técnica

En este trabajo de investigación se implementó la encuesta como técnica de recolección de datos, que permitió recabar datos tanto de delitos informáticos como de percepción de seguridad. Al respecto Feria, et al. (2020) consideran a la encuesta como una entrevista que se realiza por medio del cuestionario, este método empírico hace uso de formato impreso o digital orientado a obtener respuestas sobre el problema de investigación (ver anexo 3).

Instrumentos

Cabezas, et al. (2018, p. 123) sostiene que un cuestionario es una técnica primaria para la obtención de información basada en preguntas objetivas, coherentes y claras, que asegura que la información proporcionada por la muestra pueda ser analizada por métodos cuantitativos. El cuestionario de este informe de investigación estuvo compuesto por 22 preguntas con categorías de respuestas basadas en una escala de valoración, lo que permite realizar una medición a través de la escala de Likert. En concordancia, 11 de ellas estan relacionadas con la variable 1 (delitos informáticos) y las otras 11 concernientes a la variable 2 (percepción de seguridad), diseñadas acorde las dimensiones e indicadores descritos en la Matriz de Operacionalización de Variables (ver anexo 1).

Validez

En palabras de Villasís, et. al. (2018) cuando se habla de validez se hace referencia a lo que es verdadero o se asemeja a la verdad, es así que en una investigación los resultados son válidos cuando no posee errores, estos sesgos son aquellos que se originan por problemas metodológicos, pueden ser errores de medición, de selección o de confusión. En relación, este presente informe de investigación, fue validado por la denominada prueba por juicio de expertos, es

decir, los instrumentos que midieron las variables estudiadas; percepción de seguridad y delitos informáticos, pasaron por revisión y validación de especialistas y metodólogos, los mismos que realizaron la certificación del instrumento.

Confiabilidad

Cuando el grado de validez es alto, los resultados se denominan confiables, es decir que su proporción de error es nula o no existen sesgos (Villasís, et. al., 2018). Por lo tanto, a menor error, mayor confiabilidad. La diferencia de la confiabilidad con la validez, es que en la primera el instrumento que se usa para medir, es decir las preguntas, lo hagan de manera correcta con el menor error posible y la validez se ocupa de que el contenido de importancia para el estudio se encuentre bien representado en el instrumento (Moreno, 2017).

La determinación de confiabilidad del instrumento de esta investigación se llevó a cabo mediante el Alfa de Cronbach, este coeficiente alfa que fue detallado en 1951 por Lee Cronbach se encarga de evaluar el promedio de las correlaciones existentes entre las preguntas del instrumento (Tuapanta, et al., 2017).

Para tal caso, se realizó una prueba piloto con una muestra a 20 clientes de entidades financieras de Chimbote y Nuevo Chimbote, a quienes se le aplicará el cuestionario de ambas variables, delitos informáticos y percepción de seguridad. Después de su aplicación, se tuvo como resultado para la primera variable; 0,88 que corresponde a una confiabilidad buena, y para la segunda variable; 0,86 que equivale a una buena confiabilidad.

3.5. Procedimientos

Como primer momento, para recolectar la información el procedimiento a llevarse a cabo fue mediante la elaboración del instrumento de recolección, la encuesta. Luego se procedió a su aplicación en los sujetos de la muestra, que corresponde a los usuarios de entidades financieras de la localidad de Chimbote y Nuevo Chimbote.

Posteriormente, con la información recopilada se ordenó y sustentó en una base de datos con la finalidad de lograr un orden de resultados volcados en tablas con sus respectivos gráficos. Esto permitió cumplir el objetivo de realizar una investigación cuantitativa.

3.6. Método de análisis de datos

Para analizar los datos de esta investigación se realizó el método estadístico a través de análisis descriptivo, permitiendo indicar la información que se relaciona con la percepción de seguridad y los delitos informáticos de 4 entidades bancarias de la ciudad de Chimbote.

En consecuencia, la estadística descriptiva generó que se recopile, organice, interprete y analice los datos obtenidos de forma rápida y factible. De modo que se realice una adecuada descripción de las tablas y gráficos.

Para el análisis de los niveles de variables y dimensiones de estudio se realizó la especificación de valores que fueron descritos en la tabla de baremos, que se encuentra en anexos.

3.7. Aspectos éticos

Teniendo en cuenta la actualización del Código de Ética en Investigación de la Universidad Cesar Vallejo, del 28 de agosto del 2021, RCU N° 0262-2020; los aspectos éticos forjados en la presente investigación recurren al cumplimiento de las siguientes normativas para su desarrollo:

Artículo 3°: Principios de ética en investigación

- Autonomía; las personas participantes en este informe de investigación serán capaces de decidir por sí misma su participación o retiro de ella.
- Beneficios; la investigación procurará el bienestar de los participantes.
- Competencia profesional y científica; los autores participantes poseerán las competencias y capacidades necesarias para el desarrollo de la investigación, garantizando el rigor científico en todo su proceso de desarrollo.
- Justicia; los participantes gozarán de igual trato, sin distinción alguna.
- Libertad; los investigadores se desenvolverán en total libertad, bajo ninguna influencia política, económica, religiosa u otro tipo.
- Probidad; en la que se actuará con total honestidad en toda la investigación, incluido la presentación de resultados y respeto por los protocolos establecidos por el comité de ética.
- Respeto hacia la propiedad intelectual; por lo que el investigador respetará los derechos exclusivos pertenecientes a otros investigadores, evitando el plagio del mismo.

- Responsabilidad; en la que los investigadores asumirán con total responsabilidad y compromiso las consecuencias derivadas del proceso investigativo.
- Transparencia; la investigación será divulgada de manera que sea posible verificar la validez de los resultados de investigación y replicar su metodología.
- Precaución, se tomará en cuenta las medidas necesarias de precaución a fin de evitar repercusiones negativas futuras de la investigación.

Artículo 7°: De la publicación de las investigaciones.

- Se fomentará la autoría responsable, autor y coautor contribuirán sustancialmente al proyecto de investigación participando activamente en su desarrollo y evitando la autoría fantasma.
- Los resultados de este proyecto de investigación mantendrá en anonimato el nombre de la institución donde se realiza su estudio.

Artículo 8°: Responsabilidad del investigador.

Todo participante que esté involucrado en la investigación de acuerdo a lo exigido en el artículo 2° del presente, debe dar a conocer lo sucedido con respecto a una conducta deficiente hacia la investigación científica ante el vicerrectorado de investigación, para actuar en el caso.

Artículo 9°: De la política antiplagio.

Para su política de antiplagio la universidad Cesar Vallejo incita a realizar la originalidad de las investigaciones. Teniendo en cuenta que el plagio es considerado un delito, este proyecto de investigación presentará datos propios y recolección de información cuya fuente es citada con las normas estipuladas. Asimismo, se acredita su originalidad a través del software antiplagio detector de semejanzas que confirma que este proyecto no sobrepasa el 25% de similitud.

Por último, siendo el objeto de estudio obtener resultados reales no se realizó ninguna manipulación sobre los datos e información recolectada, lo cual infiere en su credibilidad. De igual forma la teoría y antecedentes descritos tienen la citación de su autor perteneciente.

Artículo 10°: De los Derechos del autor.

El autor tiene la autorización de difundir la investigación en publicación. Asimismo, la UCV promueve el derecho de autor y sanciona el plagio.

Artículo 11°: Del autor principal y personal investigador.

Esta investigación tuvo un autor principal liderado por Mantilla Barrón Carmen Thalia; representante del grupo. Quien asumirá la responsabilidad de la investigación que involucra su difusión y ejecución.

Artículo 12°: De las Instalaciones y equipamientos.

La instalación donde se realice la investigación respetará los protocolos de bioseguridad de manera que se garantice su buen desarrollo.

IV. RESULTADOS

Objetivo general: describir los niveles de los delitos informáticos y la percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Tabla 1

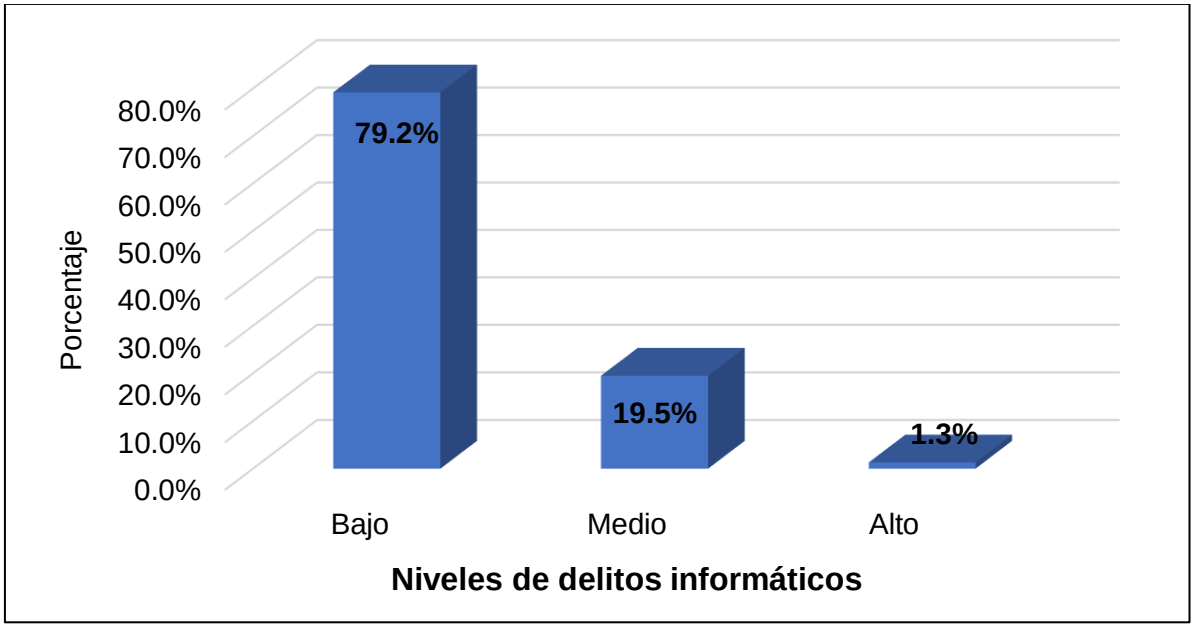
Nivel de los delitos informáticos en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Niveles	Frecuencia	Porcentaje
Bajo	304	79.2%
Medio	75	19.5%
Alto	5	1.3%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 1

Gráfico de Barras de Nivel de delitos informáticos en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Interpretación:

Los delitos informáticos en la banca digital de las entidades bancarias de Chimbote, indicaron en sus respuestas otorgadas a la encuesta que se les hizo que, tal como se observa en la tabla 1 y figura 1, el nivel de delitos informáticos ocurridos en línea en sus bancos es bajo, según el 79.2% (304 usuarios) del total de encuestados, el 19.5% respondió que el nivel de delitos ocurridos al usar la banca digital es medio y el 1.3% respondió que es bajo.

Tabla 2

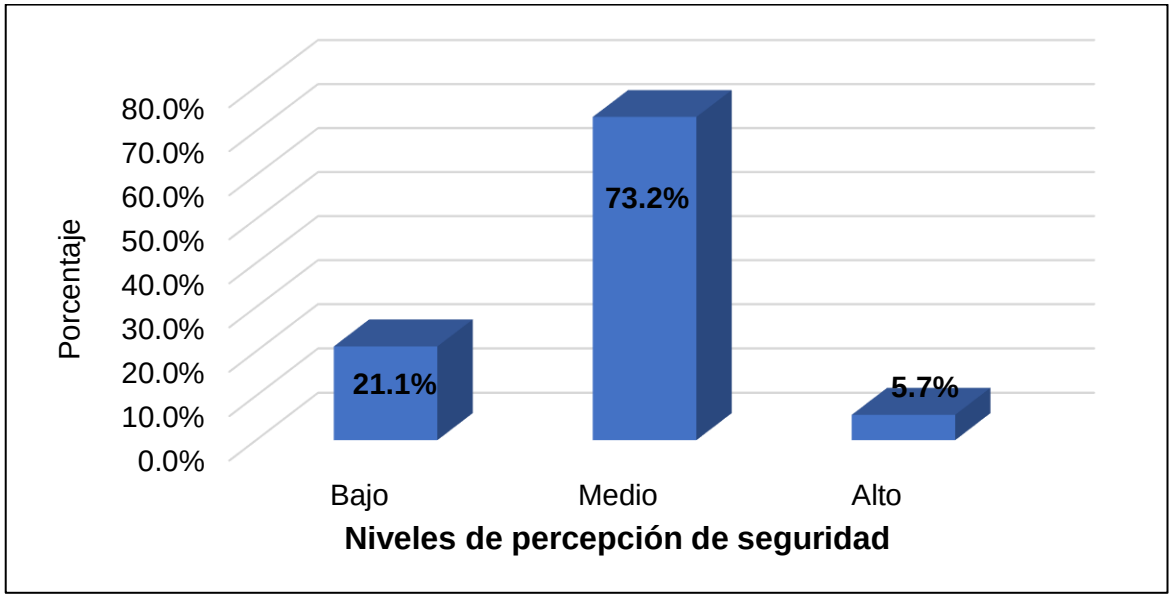
Nivel de percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Niveles	Frecuencia	Porcentaje
Bajo	81	21.1%
Medio	281	73.2%
Alto	22	5.7%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 2

Gráfico de Barras de Nivel de percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Interpretación:

La percepción de seguridad de los clientes de la banca digital de las entidades bancarias de Chimbote, según indicaron en sus respuestas otorgadas a la encuesta que se les hizo que, tal como se observa en la tabla 1 y figura 1, el nivel de seguridad de operaciones en línea en sus bancos es bajo, según el 21.1% (81 usuarios) del total de encuestados, el 73.2% respondió que el nivel de seguridad de usar la banca digital es medio y el 5.7% respondió que es bajo. Teniendo en cuenta la respuesta por mayoría en el resultado estadístico, se aprecia que la percepción de seguridad de los usuarios bancarios tiene un nivel medio con inclinación a bajo, el nivel alto queda muy alejado de su percepción; esto puede darse por causas de fraudes y estafas que se avistan de forma recurrente en las transacciones en línea, y que hoy en día se les conoce como el cibercrimen.

Objetivo específico 1: describir las modalidades de delitos informáticos recurrentes a los que se ven expuestos los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022.

Tabla 3

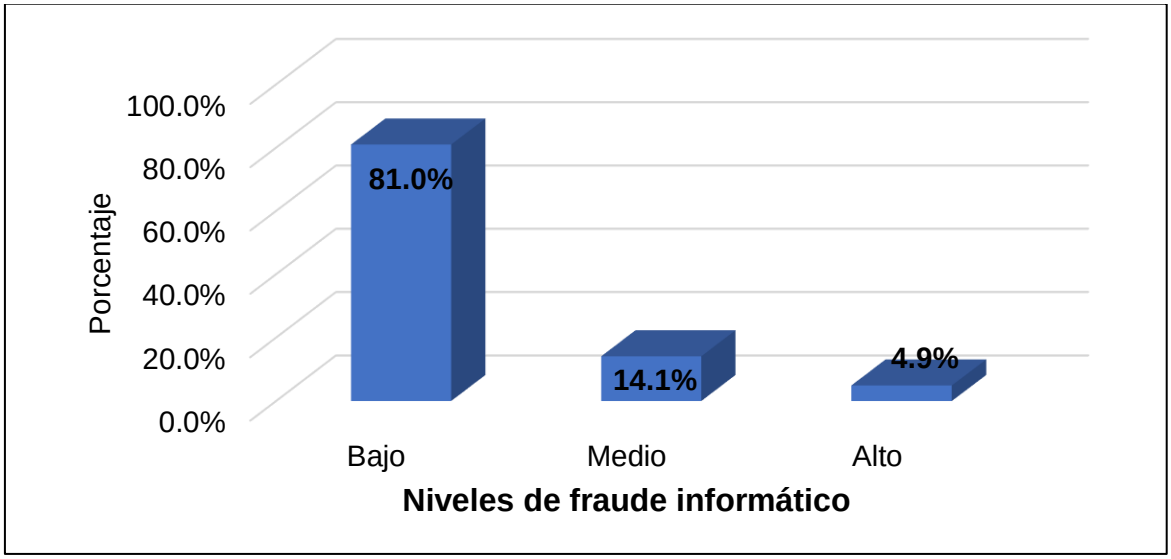
Nivel de fraude informático ocurrido en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Niveles	Frecuencia	Porcentaje
Bajo	311	81.0%
Medio	54	14.1%
Alto	19	4.9%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 3

Gráfico de Barras de Nivel de fraude informático ocurrido en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Interpretación:

Los fraudes informáticos ocurridos en la banca digital de las entidades bancarias de Chimbote, indicaron en sus respuestas otorgadas a la encuesta que se les hizo que, tal como se observa en la tabla 3 y figura 3, el nivel de fraude informático ocurrido en las operaciones en línea en sus bancos es bajo, según el 81.0% (311 usuarios) del total de encuestados, el 14.1% respondió que el nivel de fraude informático en la banca digital es medio y el 4.9% respondió que es bajo. De este modo, teniendo en consideración el valor porcentual mayor, se aprecia que el fraude informático es un tipo de delito no muy recurrente en la banca digital esto puede ser porque la banca ha podido detectar el problema y crear estrategias para aminorarlas.

Tabla 4

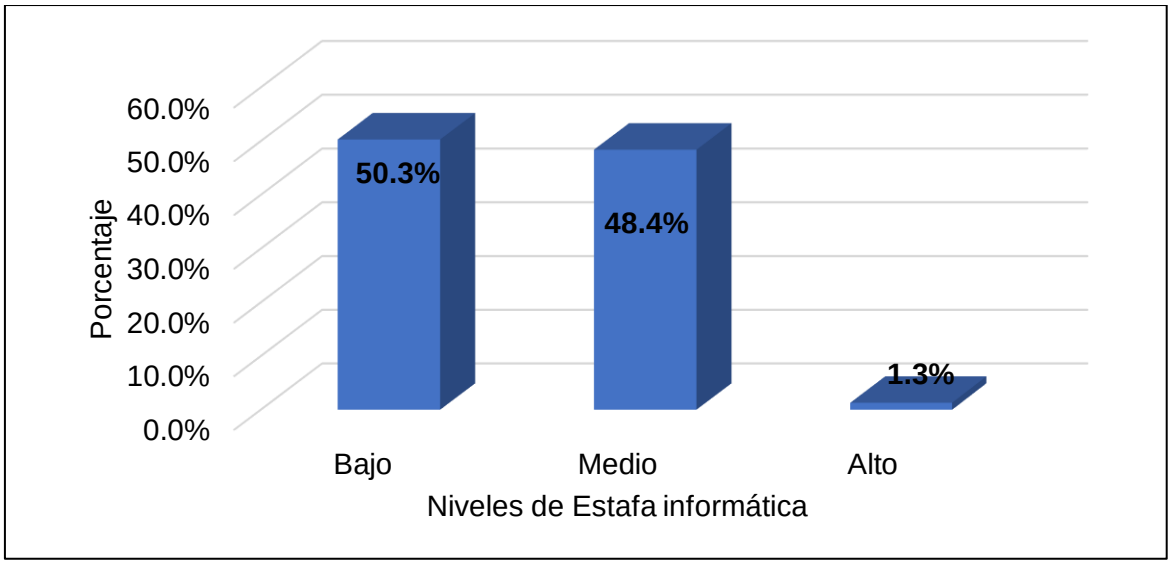
Nivel de estafas informáticas ocurridas en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Niveles	Frecuencia	Porcentaje
Bajo	193	50.3%
Medio	186	48.4%
Alto	5	1.3%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 4

Gráfico de Barras de Nivel de estafas informáticas ocurridas en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Interpretación:

Las estafas informáticas ocurridas en la banca digital de las entidades bancarias de Chimbote, indicaron en sus respuestas otorgadas a la encuesta que se les hizo que, tal como se observa en la tabla 4 y figura 4, el nivel de estafa informática ocurrido en las operaciones en línea en sus bancos es bajo, según el 50.3% (193 usuarios) del total de encuestados, el 48.4% respondió que el nivel de estafa informática en la banca digital es medio y el 1.3% respondió que es bajo.

Concluyendo que, a diferencia del fraude informático, las estafas informáticas suelen ocurrir con frecuencia en el servicio de banca digital, ya que se interpreta en el análisis estadístico que esta se localiza entre el nivel bajo (50.3%) y medio (48.4%) de frecuencia, dando lugar a inferir que este tipo de delito puede ser uno de los motivos de percepción de inseguridad que siente los usuarios para usar el servicio bancario por medio de lo digital.

Tabla 5

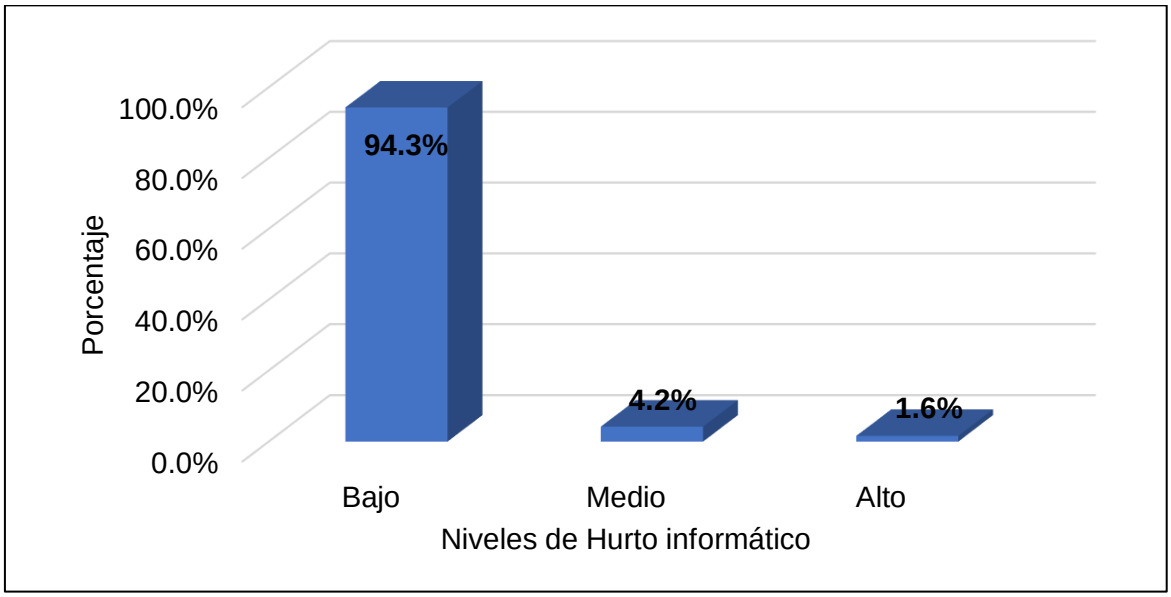
Nivel de Hurto informático ocurridas en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Niveles	Frecuencia	Porcentaje
Bajo	362	94.3%
Medio	16	4.2%
Alto	6	1.6%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 5

Gráfico de Barras de Nivel de hurtos informáticos ocurridos en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Interpretación:

Los hurtos informáticos ocurridos en la banca digital de las entidades bancarias de Chimbote, indicaron en sus respuestas otorgadas a la encuesta que se les hizo que, tal como se observa en la tabla 5 y figura 5, el nivel de hurto informático ocurrido en las operaciones en línea en sus bancos es bajo, según el 94.3% (363 usuarios) del total de encuestados, el 4.2% respondió que el nivel de hurto informático en la banca digital es medio y el 1.6% respondió que es bajo. Resultados que se interpretan como una modalidad de delito que ocurre muy pocas veces, las razones podrían ser la implementación de medidas de seguridad por parte de las entidades bancarias para disminuir ese tipo de riesgos.

Objetivo específico 2: describir el nivel de sensación de seguridad en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022.

Tabla 6

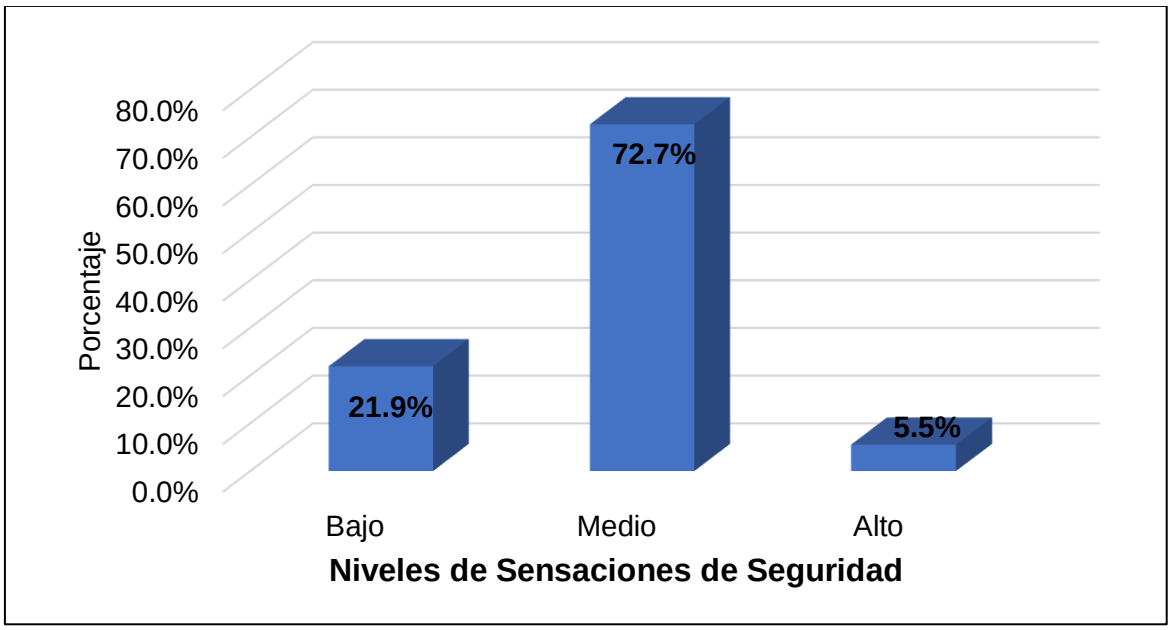
Nivel de sensaciones de seguridad percibidas por los usuarios en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Niveles	Frecuencia	Porcentaje
Bajo	84	21.9%
Medio	279	72.7%
Alto	21	5.5%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 6

Gráfico de Barras de Nivel de sensaciones de seguridad percibidas por los usuarios en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Interpretación:

Las sensaciones de seguridad percibidas por los usuarios en el uso de la banca digital de las entidades bancarias de Chimbote, indicaron en sus respuestas otorgadas a la encuesta que se les hizo que, tal como se observa en la tabla 6 y figura 6, el nivel de sensaciones de seguridad ocurrido en las operaciones en línea en sus bancos es medio, según el 72.7% (279 usuarios) del total de encuestados, el 21.9% respondió que el nivel de sensación de seguridad en la banca digital es bajo y el 5.5% respondió que es alto. Por lo tanto, respetando estos valores, se aduce que los usuarios de la banca digital perciben cierta inseguridad en su uso, el cual fluctúa entre medio a bajo; entre las tantas razones una de ellas podría ser la frecuencia de delitos digitales que se avistan en los medios de información y el interés de los bancos por ahondar en refuerzos en la creación de claves digitales, accesos o transferencias, situaciones que se han convertido en largos pasos con el objetivo de aumentar la seguridad en su uso.

Objetivo específico 3: describir el nivel de seguridad informática en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022.

Tabla 7

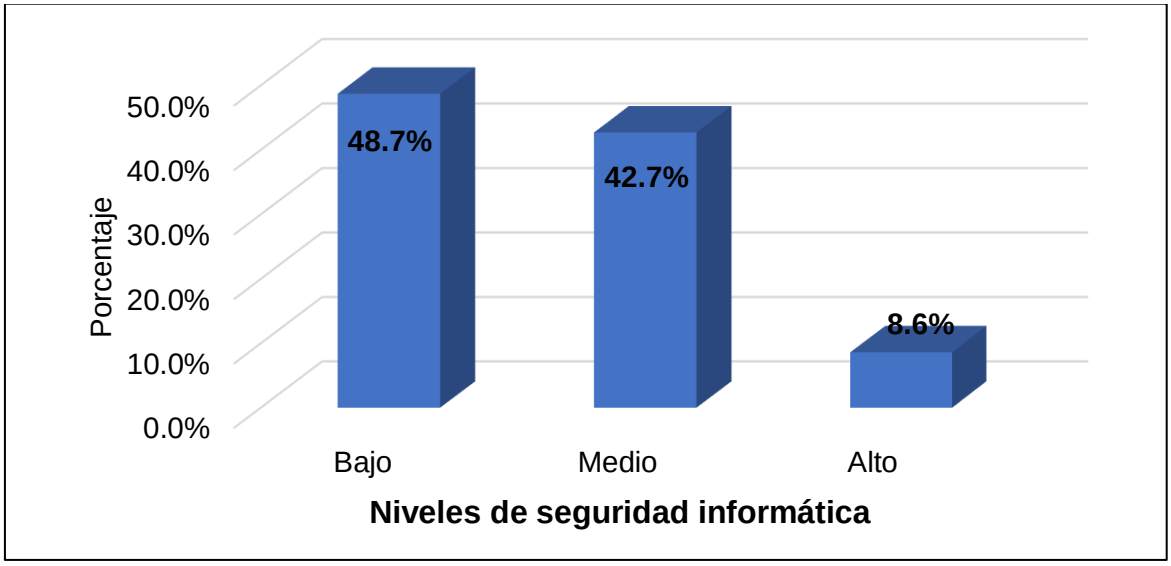
Nivel de seguridad informática percibida por los usuarios en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

Niveles	Frecuencia	Porcentaje
Bajo	187	48.7%
Medio	164	42.7%
Alto	33	8.6%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 7

Gráfico de Barras de Nivel de seguridad informática percibida por los usuarios en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Interpretación: La seguridad informática percibida por los usuarios en el uso de la banca digital de las entidades bancarias de Chimbote, indicaron en sus respuestas otorgadas a la encuesta que se les hizo que, tal como se observa en la tabla 7 y figura 7, el nivel de seguridad informática percibida en las operaciones en línea en sus bancos es bajo, según el 48.7% (187 usuarios) del total de encuestados, el 42.7% respondió que el nivel de seguridad informática de las entidades bancarias es medio y el 8.6% respondió que es alto. Por lo tanto, la seguridad informática se ubica entre medio (42.7%) y bajo (48.7), en paralelo con el resultado descrito en la tabla anterior, se atribuye que la seguridad informática que intenta entregar la banca no es totalmente óptima para los usuarios, por ello el temor duda e incertidumbre a su uso tampoco es percibida como buena.

V. DISCUSIÓN

De las evidencias anteriores, sintetizando los hallazgos principales además de su comparación con las teorías y literatura científica actual, se realiza la discusión en esta investigación.

Empezando con el objetivo general de esta investigación que se basó en describir los niveles de los delitos informáticos y la percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022, se demostró como resultado que el nivel de seguridad de las operaciones en línea de los bancos es bajo, según el 21.1% (81 usuarios) del total de encuestados, el 73.2% respondió que el nivel de seguridad de usar la banca digital es medio y el 5.7% respondió que es bajo. Teniendo en cuenta la respuesta por mayoría en el resultado estadístico, se aprecia que la percepción de seguridad de los usuarios bancarios tiene un nivel medio con inclinación a bajo, el nivel alto queda muy alejado de su percepción; esto puede darse por causas de fraudes y estafas que se avistan de forma recurrente en las transacciones en línea, y que hoy en día se les conoce como el cibercrimen. Estos resultados se inclinan a lo atribuido por Zambrano (2021) en su tesis de investigación que tuvo como objetivo establecer si la utilización y manejo de la banca móvil incentiva el aumento de delitos informáticos en la ciudad de Arequipa, por lo cual se realizó una investigación básica – cualitativa, realizando una entrevista estructurada a una muestra conformada por 10 especialistas de investigación de delitos de alta tecnología, fiscales penales, abogados y peritos en materia de delitos informáticos. Obteniendo como resultado que un 50% de los entrevistados afirman que la banca Móvil si promueve el fraude y delitos informáticos, debido a su uso masificado ha sido blanco para los ciber delincuentes, además de que también promueve la clonación de datos ya que para acceder a ella es necesario contar con datos como número de cuenta, número de tarjeta, código de seguridad y fecha de vencimiento de la tarjeta. Teóricamente se sustenta en Ávalos (2021, p.12) quien manifiesta que el delito informático, en un sentido estricto, engloba cualquier comportamiento ilegal que sitúe en peligro la seguridad de los sistemas informáticos y el procesamiento de datos a través de operaciones electrónicas. Además, Temperini (2018, p. 53) infiere que la tecnología es una especie de potenciador de este tipo de delitos, pues el crimen no es nuevo, sino que al

combinarse con ciertas características de las nuevas tecnologías terminan llevando al delito a un nuevo nivel.

El objetivo específico 1 se encargó de describir las modalidades de delitos informáticos recurrentes a los que se ven expuestos los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022. En relación a la modalidad de delito informático denominada “fraude informático”, los resultados arrojaron que el nivel de fraude informático ocurrido en las operaciones en línea de los bancos es bajo, según el 81.0% (311 usuarios) del total de encuestados, asimismo el 14.1% respondió que el nivel de fraude informático en la banca digital es medio y el 4.9% respondió que es bajo. De este modo, teniendo en consideración el valor porcentual mayor, se aprecia que el fraude informático es un tipo de delito no muy recurrente en la banca digital esto puede ser porque la banca ha podido detectar el problema y crear estrategias para aminorarlas. De manera similar, los delitos informáticos ocasionados por las “estafas informáticas” según los resultados de las encuestas suelen ocurrir con frecuencia en el servicio de banca digital, ya que se interpreta en el análisis estadístico que esta se localiza entre el nivel bajo (50.3%) y medio (48.4%) de frecuencia, dando lugar a inferir que este tipo de delito puede ser uno de los motivos de percepción de inseguridad que siente los usuarios para usar el servicio bancario por medio de lo digital. Respecto a la última modalidad de delito que se denomina “hurto informático” los resultados indicaron que se encuentra en un nivel bajo según el 94.3%, lo que conlleva a interpretarlo como como una modalidad de delito que ocurre muy pocas veces, las razones podrían ser la implementación de medidas de seguridad por parte de las entidades bancarias para disminuir ese tipo de riesgos. Estos resultados se complementan con el estudio realizado por Angulo y Córdova (2019) que tuvo como objetivo diseñar un plan estratégico para ayudar en las medidas de precaución de los delitos informáticos en las entidades bancarias ecuatorianas, realizó una investigación de campo de tipo descriptivo, en donde se encuestaron a un total de 60 personas, donde 50 fueron clientes de bancos, 8 expertos informáticos y 2 expertos en delitos informáticos. Los resultados demostraron que un 68% de los encuestados han sido afectados por robo de identidad. De este total, el 86% afirma que fue mediante páginas web. Asimismo, el 30% de ellos no obtuvo solución al problema. Concluyendo que es necesaria la

puesta en marcha de procedimientos internos como proceso de: recuperación, de operación alterna y de restauración, además de capacitar permanentemente a clientes de bancos y a los administradores de justicia en temas de prevención y precaución de los delitos en las instituciones bancarias, puesto que él 70% de los encuestados considera que el banco del cual es cliente no es seguro en relación a este tipo de delitos. Ambos estudios, la realizada en esta investigación y la de Angulo y Córdova, concuerdan en que la estafa informática es el delito informático que más prevalece en las entidades bancarias, siendo el fraude por medio de páginas web la que predomina en la banca digital, o también conocido como smishing, que en palabras de Elif & Bagriyanik (2020) el smishing es una modalidad de estafa realizada a través de mensajes de texto o SMS, haciendo uso de URL abreviado y con alias como por ejemplo Bitly, en donde se hacen pasar por fuentes confiables de bancos para engañar y obtener información personal.

De acuerdo al objetivo específico 2, que describió los niveles de sensaciones de seguridad en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022, en sus resultados el nivel de sensaciones de seguridad ocurrido en las operaciones en línea en sus bancos es medio, según el 72.7% (279 usuarios) del total de encuestados, el 21.9% respondió que el nivel de sensación de seguridad en la banca digital es bajo y el 5.5% respondió que es alto. Por lo tanto, respetando estos valores numéricos, se aduce que los usuarios de la banca digital perciben cierto, temor, duda, incertidumbre e inseguridad en su uso, el cual fluctúa entre regular a poco; entre las tantas razones una de ellas podría ser la frecuencia de delitos digitales que se avistan en los medios de información y el interés de los bancos por ahondar en refuerzos en la creación de claves digitales, accesos o transferencias, situaciones que se han convertido en largos pasos con el objetivo de aumentar la seguridad en su uso. Para profundizar estos resultados se compara con el estudio realizado por Guerrero y Castillo (2017) que tuvo como objetivo de investigación analizar y comprender tanto el contexto como los tipos de ciberdelitos cometidos en el sector financiero, para generar tácticas que favorezcan a su prevención y tipificación en base a la legislación vigente de manera nacional como internacional. Su investigación fue de tipo descriptiva y su diseño de investigación documental. Dada su

investigación, concluyó que en Colombia las denuncias por ciberdelitos han aumentado en un 25% más respecto a los delitos por homicidios y narcotráficos. Por otro lado, un 75% de los ciberdelitos reportados son asociados al Sistema Financiero, destacando el phishing como el principal ataque, resaltando que estos delitos no se realizan por medio de aparatos tecnológicos sofisticados, sino que es ejecutado mediante correos electrónicos y aplicaciones móviles. Datos interesantes que posibilitan comparar los tipos de delitos más recurrentes que suceden en la banca digital, es así que en esta investigación y el estudio de Guerrero y Castillo argumentan que los tipos de delitos habituales son el pishing (por correo electrónico) y smishing (por mensaje de texto), aunque en esta investigación prevalece el smishing y la investigación en comparación el pishing. No esta demás resaltar que esta diferencia puede atribuirse a causales como el contexto geográfico, y el año de estudio; en esta investigación se desarrolla en Perú en el 2021, y el estudio de Guerrero y Castillo en Colombia en el 2017. En efecto, se asume que luego de la llegada de la pandemia que envolvió al mundo entero, Covid 19, el uso de la banca digital aumento vertiginosamente así mismo los riesgos y delitos ocurridos en ella. Estos estudios se sustentan en la teoría de Jensen (2017) quien argumentó que una de las maneras de evitar ser engañado bajo estas modalidades es la capacitación, en un trabajo de investigación en Estados Unidos bajo un estudio de campo comprobó que las personas que tuvieron capacitación respecto a los ataques de pishing pudieron detectar y evitar de una mejor forma los ataques en relación con los que no habían sido capacitados.

Por último, el objetivo específico 3 se encargó de describir los niveles de seguridad informática en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022, la data de los resultados demostró que el nivel de seguridad informática percibida en las operaciones en línea en sus bancos es bajo, según el 48.7% (187 usuarios) del total de encuestados, el 42.7% respondió que el nivel de seguridad informática de las entidades bancarias es medio y el 8.6% respondió que es alto. Por lo tanto, la seguridad informática se ubica entre medio (42.7%) y bajo (48.7), en paralelo con el resultado descrito en la tabla anterior, se atribuye que la seguridad informática que intenta entregar la banca no es totalmente óptima para los usuarios, por ello

el temor duda e incertidumbre a su uso tampoco es percibida como buena. Este análisis es atribuible amplificarlo con el estudio realizado por Córdova y Barios (2018) que tuvo por objetivo analizar cómo impacta de manera operacional, financiera y de imagen corporativa el aumento de los delitos informáticos en dos bancos importantes de Lima Metropolitana como son el Banco de Crédito del Perú y BBVA en los últimos 5 años. Realizó una investigación cualitativa, descriptiva; entrevistó a 23 personas que constaron de 13 clientes y 10 trabajadores de las respectivas entidades. El instrumento de investigación utilizado fue el cuestionario. En torno a los resultados se identificó que por día se realizan entre 12 a 20 reclamos por fraudes, lo que corresponde a un aumento del 600% ya que años atrás se suscitaban 2 reclamos diariamente como máximo. En consecuencia, el número de trabajadores analistas de fraude en los bancos también se han duplicado de 2 a 4 colaboradores. En conclusión, se argumentó que, las entidades financieras han tratado de optimizar y cambiar sus estrategias operativas para desempeñarse en el cumplimiento de prevención, localización y monitoreo de estos fraudes, implementando dispositivos de seguridad, como el caso de BCP con el “Token” incorporado a sus plataformas, puesto que, a nivel nacional se reportaron hasta 16 millones de transacciones bancarias correspondiéndole a la entidad financiera el 50% de ellas. En conclusión, la información descrita en ambas investigaciones tiene congruencia y se relacionan de forma directa en el sentido que en esta tesis se percibe que la seguridad informática que proporciona la banca digital y el sentimiento de los usuarios envueltos por la duda, desconfianza, incertidumbre e inseguridad en sus transacciones digitales es de un nivel medio, que quiere decir que no se encuentran totalmente satisfechos ni conformes con su uso, dada esta realidad las causas son asumidas por la tesis de Córdova y Barios quienes describen que los fraudes informáticos han aumentado en un 600% en los últimos años, situación que ha hecho que los bancos traten de optimizar sus estrategias de prevención y monitoreo de fraudes informáticos. No está de más agregar que si el uso de la banca digital ha aumentado, es natural que los riesgos digitales también estén transitando ese auge, y la seguridad e inseguridad que percibe el usuario consumidor dependa del número de delitos que se generen en el uso del servicio. Esta realidad se sustenta en la teoría de la página de noticias Verified News

Explorer Network (2021) mediante un estudio de la empresa IPSOS menciona que, en Chile, la percepción de inseguridad de los clientes de instituciones financieras es muy alta puesto que 3 de cada 4 usuarios de bancos que corresponde al 75% han recibido correos o mensajes de texto considerados una amenaza de fraude cibernético y llamadas telefónicas con intención de robo de información. además de que 1 de cada 4 clientes ha sido víctima de fraude por clonación o uso fraudulento de medio de pago por tarjeta de crédito o débito, donde más del 25% ha vivido esta situación más de una vez. Asimismo, Santisteban, Ocares & Andrade (2020), agregan que se gastan millones de dólares en todo el mundo para prevenir los ciberataques, pero a menos que las organizaciones trabajen de manera integral, estas amenazas seguirán perturbando las operaciones de las entidades.

VI. CONCLUSIONES

1. Empezando con el objetivo general de esta investigación que se basó en describir los niveles de los delitos informáticos y la percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022, se demostró como resultado que el nivel de seguridad de las operaciones en línea de los bancos es bajo, según el 21.1% (81 usuarios) del total de encuestados, el 73.2% respondió que el nivel de seguridad de usar la banca digital es medio y el 5.7% respondió que es bajo. Teniendo en cuenta la respuesta por mayoría en el resultado estadístico, se aprecia que la percepción de seguridad de los usuarios bancarios tiene un nivel medio con inclinación a bajo, el nivel alto queda muy alejado de su percepción; esto puede darse por causas de fraudes y estafas que se avistan de forma recurrente en las transacciones en línea, y que hoy en día se les conoce como el cibercrimen.
2. El objetivo específico 1 se encargó de describir las modalidades de delitos informáticos recurrentes a los que se ven expuestos los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022. En relación a la modalidad de delito informático denominada “fraude informático”, los resultados arrojaron que el nivel de fraude informático ocurrido en las operaciones en línea de los bancos es bajo, según el 81.0% (311 usuarios) del total de encuestados, asimismo el 14.1% respondió que el nivel de fraude informático en la banca digital es medio y el 4.9% respondió que es bajo. De este modo, teniendo en consideración el valor porcentual mayor, se aprecia que el fraude informático es un tipo de delito no muy recurrente en la banca digital esto puede ser porque la banca ha podido detectar el problema y crear estrategias para aminorarlas. De manera similar, los delitos informáticos ocasionados por las “estafas informáticas” según los resultados de las encuestas suelen ocurrir con frecuencia en el servicio de banca digital, ya que se interpreta en el análisis estadístico que esta se localiza entre el nivel bajo (50.3%) y medio (48.4%) de frecuencia, dando lugar a inferir que este tipo de delito puede ser uno de los motivos de percepción de inseguridad que siente los usuarios para usar el servicio bancario por medio de lo digital. Respecto a la última modalidad de delito que se denomina “hurto informático” los resultados

indicaron que se encuentra en un nivel bajo según el 94.3%, lo que conlleva a interpretarlo como una modalidad de delito que ocurre muy pocas veces, las razones podrían ser la implementación de medidas de seguridad por parte de las entidades bancarias para disminuir ese tipo de riesgos.

3. De acuerdo al objetivo específico 2, que describió los niveles de sensaciones de seguridad en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022, en sus resultados el nivel de sensaciones de seguridad ocurrido en las operaciones en línea en sus bancos es medio, según el 72.7% (279 usuarios) del total de encuestados, el 21.9% respondió que el nivel de sensación de seguridad en la banca digital es bajo y el 5.5% respondió que es alto. Por lo tanto, respetando estos valores, se aduce que los usuarios de la banca digital perciben cierto, temor, duda, incertidumbre e inseguridad en su uso, el cual fluctúa entre regular a poco; entre las tantas razones una de ellas podría ser la frecuencia de delitos digitales que se avistan en los medios de información y el interés de los bancos por ahondar en refuerzos en la creación de claves digitales, accesos o transferencias, situaciones que se han convertido en largos pasos con el objetivo de aumentar la seguridad en su uso.
4. Por último, el objetivo específico 3 se encargó de describir los niveles de seguridad informática en la percepción de los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022, la data de los resultados demostró que el nivel de seguridad informática percibida en las operaciones en línea en sus bancos es bajo, según el 48.7% (187 usuarios) del total de encuestados, el 42.7% respondió que el nivel de seguridad informática de las entidades bancarias es medio y el 8.6% respondió que es alto. Por lo tanto, la seguridad informática se ubica entre medio (42.7%) y bajo (48.7), en paralelo con el resultado descrito en la tabla anterior, se atribuye que la seguridad informática que intenta entregar la banca no es totalmente óptima para los usuarios, por ello el temor duda e incertidumbre a su uso tampoco es percibida como buena.

VII. RECOMENDACIONES

1. Se recomienda, al gerente de las entidades bancarias en general hacer una investigación de mercado para identificar el nivel de conocimiento de los usuarios sobre las medidas de seguridad a tener en cuenta cuando usan la banca electrónica, como es: la configuración de una contraseña segura, la identificación de una dirección URL correcta, verificación del candado de seguridad de la página, reconocimiento de web falsos, entre otras cuestiones. Las cuales ayudaran a identificar cuanto saben o ignoran los usuarios sobre un uso correcto, seguro y adecuado de la banca electrónica para que las entidades tomen acciones dirigidas a brindar información precisa al usuario empleando distintas estrategias como la frecuencia de las publicidades informativas o por mensajes de texto que eduquen a los consumidores para un uso correcto y seguro del servicio de banca digital.
2. Se recomienda al gerente de las entidades bancarias, que estudien la posibilidad de hacer uso de la identificación biométrica facial, así como también la identificación por medio de la huella, conocida como dactilar; requisito que debe exigirse cada vez que se utiliza las aplicaciones que ofrece la banca móvil y no solamente, como sucede en la actualidad, cuando ha ocurrido señales o errores como olvidos de contraseñas, pérdida de tarjeta, entre otros.
3. Se recomienda al área gerencial encargado de la gestión de la banca móvil de las entidades bancarias, realizar un permanente tratamiento a los tipos de delitos informáticos que prevalecen en la banca digital, con el objetivo de generar estrategias que puedan amortiguar los problemas consecuentes de forma rápida o en el menor tiempo posible, para disminuir el número de afectados.
4. Se recomienda a las entidades bancarias, invertir en investigación y desarrollo en cuanto a software y equipos especializados, es decir, estar a la vanguardia con lo último en tecnología e ir por delante de los delincuentes digitales con la finalidad de disminuir la vulnerabilidad de seguridad en los usuarios.

REFERENCIAS

Agencia EFE. (31 de agosto del 2021). *Los ciberataques en Latinoamérica han aumentado un 24 % este año*. https://www.efe.com/efe/america/tecnologia/los-ciberataques-en-latinoamerica-han-aumentado-un-24-este-ano/20000036-4619548

Aguilar, A. (7 de diciembre de 2020). *Los delitos informáticos ocasionaron en 2019 pérdidas superiores al 1% del PIB mundial, por encima de los 800.000 millones de euros.* Business Insider. https://www.businessinsider.es/impacto-ciberdelitos-ya-superior-1-pib-mundial-768519

Alburqueque, E. (2018). *Percepción sobre calidad del servicio y satisfacción del alumno en el área de finanzas, UCV-Piura, año 2016*. [Tesis de titulación, Universidad Nacional de Piura, Piura, Perú]. Repositorio UNP. https://repositorio.unp.edu.pe/bitstream/handle/UNP/2082/ADM-ALB-DIO-2018.pdf?sequence=1&isAllowed=y

Ali, G., Mussa, A., & Sam, A. (2020). Evaluation of key security issues associated with mobile money systems in uganda. *Information, 11*(6), 1-24. http://dx.doi.org/10.3390/info11060309

Allassani, W. (2017). Determining factors of bank employee reading habits of information security policies. *Journal of Information Systems and Technology Management, 11*(3), 533-548. Universidad de Sao Paulo. https://www.redalyc.org/articulo.oa?id=203232705003

Álvarez, A. (2021). *Clasificación de las investigaciones*. Universidad de Lima. https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10818/Nota%20Acad%c3%a9mica%202%20%2818.04.2021%29%20-%20Clasificaci%c3%b3n%20de%20Investigaciones.pdf?sequence=4&isAllowed=y

Andrade, R., Ortiz, I., & Cazares, M. (2020, 28 de julio). *Cybersecurity attacks on smart home during Covid-19 pandemic.* [ponencia]. Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, London, UK. https://doi.org/10.1109/WorldS450073.2020.9210363

Angulo, J. y Córdova, M. (2020). *Análisis de la taxonomía de los delitos informáticos en el sector bancario del Ecuador 2014 – 2019*. [Tesis para

Título profesional, Universidad de Guayaquil, Guayaquil, Ecuador]. Repositorio Institucional. http://repositorio.ug.edu.ec/handle/redug/44411

Asociación de Bancos del Perú (2020). El 38% de los montos de fraudes en tarjetas en 2020 fueron por internet, según Asbanc. *Revista El Comercio.* https://elcomercio.pe/economia/peru/el-38-de-los-montos-de-fraudes-en-tarjetas-en-2020-fueron-por-internet-segun-asbanc-nndc-noticia/?ref=ecr

Ausecha, H. et al. (2021). Safe-pro: herramienta de entretenimiento y aprendizaje en seguridad informática. *Revista Ibérica De Sistemas e Tecnologias De Informação*, *1*(41), 289-302. https://www.proquest.com/scholarly-journals/safe-pro-herramienta-de-entretenimiento-y/docview/2493870027/se-2

Ávalos, Z. (2021). *Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada*. (Informe de Análisis N° 34). Oficina de Análisis Estratégico Contra La Criminalidad. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1667473-ciberdelincuencia-en-el-peru-pautas-para-su-investigacion-fiscal-especializada

Bokovnya, A., et al. (2020). Computer crimes on the COVID-19 scene: analysis of social, legal, and criminal threats. *Cuestiones Políticas, vol.38*, (1), 463-478. https://produccioncientificaluz.org/index.php/cuestiones/article/view/34339/36193

Boletín Oficial del Estado. (2017). *Prevención de riesgos laborales.* https://www.diba.cat/documents/467843/122049749/Codi_Prevencion_de_riesgos_laborales.pdf/c56dadda-f618-40ec-b8d4-79808719d255

Cabezas, E., Naranjo, D. y Torres, J. (2018). *Introducción a la Metodología de la Investigación Científica.* Universidad de las Fuerzas Armadas ESPE. http://repositorio.espe.edu.ec/jspui/bitstream/21000/15424/1/Introduccion%20a%20la%20Metodologia%20de%20la%20investigacion%20cientifica.pdf

Cardich, G. (2020). La auditoría forense y su incidencia en la gestión de riesgo *de fraude de las cajas municipales de ahorro y crédito en el Perú, 2016-2017.* (Tesis de Maestría, Universidad San Martin de Porres, Lima, Perú). Repositorio Institucional

https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/6615/cardich_cg.pdf?sequence=3&isAllowed=y

Chavarro, L. (2018). Riesgo e incertidumbre como características de la sociedad actual: ideas, percepciones y representaciones. *Revista Reflexiones, vol. 97,* (1), 65-75. https://www.redalyc.org/journal/729/72955555005/html/

Cherniavskyi, S. et al. (2021). Measures to combat cybercrime: analysis of international and Ukrainian experience. *Cuestiones Políticas, vol.39*, (69), 115-132. https://doi.org/10.46398/cuestpol.3969.06

Chiavenato, I. (2017). *Planeación estratégica: fundamentos y aplicaciones*. (3ra. ed.). McGraw-Hill. https://www.remax-accion.com.ar/wp-content/uploads/2021/04/127-Planeacion-estrategica-fundametos-chiavenato-idalberto.pdf

Chiavenato, I. (2019). *Introducción a la teoría general de la administración.* file:///C:/Users/USER/Downloads/dokumen.pub_introduccion-a-la-teoria-general-de-la-administracion-decima-edicion-9781456269821-1456269828-9781456271824-1456271822%20(1).pdf

Córdova, N y Barios, R. (2018). *Análisis de los principales factores financieros, operacionales y de reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú como son Banco de crédito del Perú y Banco Continental en los últimos 5 años.* (Tesis para Licenciatura, Universidad Peruana de Ciencias Aplicadas, Lima, Perú). Repositorio Institucional. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625668/Aroni_cn.pdf?sequence=1&isAllowed=y

Corti, H. (2016). Normas y aparatos conceptuales: dos aspectos del derecho a partir de la lectura de una frase de Alchourrón y Bulygin. *Revista de Teoría y Filosofía del Derecho*, (45), 141-188. https://www.redalyc.org/journal/3636/363648284006/html/

Díaz, N. (2016). *Población y muestra.* http://ri.uaemex.mx/bitstream/handle/20.500.11799/63099/secme26877.pdf?sequence=1

Elif, U. & Bagriyanik, M. (2020). The effect of SMiShing attack on security of demand response programs. *Energies, 13*(17), 45-42. http://dx.doi.org/10.3390/en13174542

Federal Bureau of Investigation (2020). *Internet crime report 2020*. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Feria, H., Matilla, M. y Mantecón, S. (2020). La entrevista y la encuesta: ¿métodos o técnicas de indagación empírica? *Didáctica y Educación, vol. XI,* (3), 62-79. http://revistas.ult.edu.cu/index.php/didascalia/article/view/992/997

Guerrero, B. y Castillo, D. (2017). *Desafíos técnicos y Jurídicos frente al ciberdelito en el sector bancario colombiano.* (Tesis para titulación, Universidad Nacional Abierta y a Distancia, Colombia). Repositorio Institucional. https://repository.unad.edu.co/bitstream/handle/10596/13387/52498805.pdf?sequence=5&isAllowed=y

Hassani, H. et. al. (2021). Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443. *Procedia Computer Science, vol. 191*, (2021),33-40. https://www.sciencedirect.com/science/article/pii/S1877050921014009?via%3Dihub

Hossein, S. et. al. (2021). Directed adversarial sampling attacks on phishing detection. *Journal of Computer Security, vol. 29*, (1), 1-23. https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=25b95098-92e0-4ebc-8b98-bf248037ba3b%40pdc-v-sessmgr02

Inei, (2017). *Áncash, Resultados definitivos*. Instituto Nacional de Estadística e Informática. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1552/02TOMO_01.pdf

Jacome, N. y Villamizar, C. (2019). Computer technique for the suitability of digital evidence in attacking an information system: Forensic analysis for the digital custody chain. *Journal of Physics: Conference Series, 1388*, (1). 1-6.

https://www.proquest.com/docview/2568382837/fulltextPDF/85E5CB7A2DF84A0CPQ/37?accountid=37408

Jensen, M. et. al. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Revista de Sistemas de Información de Gestión, vol. 34*, (2), 597-626. https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=6d1e400f-07cf-4653-a45d-59f9efedac7d%40redis

Mayer, L. y Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. Revista Chilena de Derecho y Tecnología. vol. 9, (1), 151-184. https://scielo.conicyt.cl/pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf

Moreno, A. (2017). *La rigurosidad científica: validez y confiabilidad en los paradigmas cuantitativo y cualitativo*. file:///C:/Users/USER/Downloads/169-Texto%20del%20art%C3%ADculo-224-1-10-20210818.pdf

Mori, F. (2019). *Los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima, periodo 2008 Al 2012.* (Tesis de Maestría, Universidad Nacional Federico Villareal, Lima, Perú). Repositorio UNFV. http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/3519/UNFV_MORI_QUIROZ_FRANCISCO_MAESTRIA_2019%20%283%29.pdf?sequence=1&isAllowed=y

Mugarza, I., Flores, J. & Montero, J. (2020). Security Issues and Software Updates Management in the Industrial Internet of Things. *Sensors, 20*(24), 1-22. https://doi.org/10.3390/s20247160

Najar, J. & Alemán, H. (2017). Technology and bank fraud. *Visión electrónica, vol. 11*, (2), 1-11. https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=c4748cdc-613a-4456-9337-2edba6e13ac5%40pdc-v-sessmgr02

Nicomedes, E. (2018). *Tipos de investigación*. https://core.ac.uk/download/pdf/250080756.pdf

O'Leary, D. (2019). What Phishing E-mails Reveal: An Exploratory Analysis of Phishing Attempts Using Text Analysis. *Journal of information systems, vol. 33*, (3), 285-307. https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=a6a26ae0-1e6f-4817-8019-b63cfe474742%40sessionmgr103

Optical Networks. (3 de agosto de 2018). *Alerta en las entidades públicas peruanas por incremento de ciberataques.* https://www.optical.pe/blog/alerta-en-las-entidades-publicas-peruanas-por-incremento-de-ciberataques/

Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*. Revista Criminalidad, 62*(2),199-217. https://biblat.unam.mx/hevila/Revistacriminalidad/2020/vol62/no2/5.pdf

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.* (Tesis de maestría, Universidad Cesar Vallejo, Lima, Perú). Repositorio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Parraguez, L. y Caldera, E. (junio, 2016). Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection. Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection. *OASIS, 2016*, (24),109-128. https://www.redalyc.org/journal/531/53163716007/

Pichihua, S. (21 de enero del 2021). Cada mes hay más de 300 denuncias por delitos informáticos. *Andina.* https://andina.pe/agencia/noticia-cada-mes-hay-mas-300-denuncias-delitos-informaticos-830617.aspx

Revista Gana Más. (27 de septiembre de 2019). Ciberseguridad: El 90% de las entidades financieras de la región fueron atacadas. Revista Gana Más. https://revistaganamas.com.pe/ciberseguridad-el-90-de-las-entidades-financieras-de-la-region-fueron-atacadas/

Ríos, M. (03 de agosto de 2020). Advierten incremento de delitos informáticos. *Diario El Correo.* https://diariocorreo.pe/edicion/chimbote/advierten-incremento-de-delitos-informaticos-946649/

Rodríguez, O. (2020). *Análisis de los delitos informáticos en base a la alteración y modificación mediante transferencia electrónica en modalidad tarjeta de crédito*. (Tesis de titulación, Universidad Laica Vicente Rocafuerte, Guayaquil, Ecuador). Repositorio Institucional. http://repositorio.ulvr.edu.ec/bitstream/44000/4146/1/T-ULVR-3450.pdf

Sánchez, B. et, al. (diciembre, 2017). Smart Campus: Trends in cybersecurity and future development. *Revista Facultad de Ingeniería, 27*, (47), 93-101. https://www.redalyc.org/articulo.oa?id=413957694009

Sánchez, M. (2018). *La Percepción de seguridad y la realidad Social. Kriptoningenieros.* http://www.kriptoningenieros.com/Documentos/Articulo_seg_1.pdf

Santisteban, A., Ocares, L. & Andrade, L. (2020). Analysis of National Cybersecurity Strategies. *International Journal of Advanced Computer Science and Applications, vol. 11*, (12), 711-779. https://thesai.org/Downloads/Volume11No12/Paper_88-Analysis_of_National_Cybersecurity_Strategies.pdf

Téllez, J. (2008). *Derecho Informático*. McGraw Hill. https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

Temperini, M. (2018). *Delitos Informáticos y Cibercrimen: Alcances, Conceptos y Características.* Erreius. http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Tuapanta, J., Duque, M. y Mena, A. (2017). Alfa de Cronbach para validar un cuestionario de uso de TIC en docentes universitarios. *Revista mktDescubre, 2017*, (10), 37 - 48. https://www.researchgate.net/profile/Miguel-Duque-3/publication/331332628_ALFA_DE_CRONBACH_para_validar_un_cuestionario_de_uso_de_TIC_en_docentes_universitarios/links/5c746a34458515831f6fe123/ALFA-DE-CRONBACH-para-validar-un-cuestionario-de-uso-de-TIC-en-docentes-universitarios.pdf

Vargas, J. (28 de octubre del 2019). *Perú: el sistema financiero deja cinco mil afectados al día*. Ojo Público. https://ojo-publico.com/1431/peru-el-sistema-financiero-deja-cinco-mil-afectados-al-dia

Ventura, J. (2017). ¿Población o muestra? Una diferencia necesaria. *Revista Cubana de Salud Pública, vol.43*, (3), 648-349. http://scielo.sld.cu/scielo.php?pid=s0864-34662017000400014&script=sci_arttext&tlng=en

Villón, H., et al. (2019). Pharming y phishing: Delitos informáticos penalizados por la legislación ecuatoriana. *Revista Ibérica De Sistemas e Tecnologías De Informação, 2019,* (E17), 671-677. https://www.proquest.com/scholarly-journals/pharming-y-phishing-delitos-informáticos/docview/2195127299/se-2

Villasís, M., et. al. (2018). El protocolo de investigación VII. Validez y confiabilidad de las mediciones. *Revista alergia México, vol. 65*, (4), 414-421. http://www.scielo.org.mx/scielo.php?pid=S2448-91902018000400414&script=sci_arttext

Verified News Explorer Network. (9 de septiembre de 2021). *Fraudes en servicios financieros: uno de cada cuatro clientes ha sido víctima de un engaño*. https://vnexplorer.net/fraudes-en-servicios-financieros-uno-de-cada-cuatro-clientes-ha-sido-victima-de-un-engano-ez2021414302.html

Zambrano, A. (2021). *El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020.* (Tesis de titulación, Universidad Cesar Vallejo, Arequipa, Perú). Repositorio Institucional https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62306/Zambrano_GAA-SD.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1. Matriz de operacionalización de variable

Variables de estudio	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Escala de medición
Variable 1: Delitos Informáticos	Actos que ponen en peligro o dañan la integridad, confidencialidad y/o disponibilidad de datos y sistemas informáticos, por medio de aparatos tecnológicos, aplicaciones móviles, transacciones electrónicas, etc., vulnerando a personas, empresas y gobiernos (Ospina y Sanabria, 2020)	Acciones ilícitas que transgreden y roban información personal por medio de sistemas informáticos o tecnologías de la información para suplantar la identidad de otra persona y cometer algún perjuicio en su contra, ya sea material o moral.	Fraude informático	Fraude al Sistema	1	Ordinal
				Fraude en los Datos	2	
			Estafa informática	Phishing	3,4	
				Smishing	5,6	
				Vishing	7,8	
			Hurto informático	Hurto Sistemático	9,10	
				Hurto de Valores	11	
Variable 2: Percepción de seguridad	Todo aquello que mide la sensación de la persona frente a condiciones de seguridad o inseguridad en el entorno donde se desenvuelve, desde el punto emocional en donde intervienen el miedo, rabia, ansiedad, etc., así como desde el punto institucional en base al desconocimiento, desconfianza, incertidumbre, etc. (Sánchez, 2018)	Aquellas sensaciones o emociones de las personas en determinadas situaciones, donde un conjunto de acciones hacen que se sienta más o menos seguro.	Niveles de seguridad	Seguro (alto)	12,13	Ordinal
				Dudoso (medio)	14	
				Peligroso (bajo)	15	
			Sensaciones de seguridad	Confianza	16	
				Incertidumbre	17	
				Amenaza	18	
			Seguridad informática	Prevención de riesgos	19	
				Políticas	20	
				Aspectos Normativos	21,22	

Anexo 2. Instrumento de recolección de datos

CUESTIONARIO PARA MEDIR LA VARIABLE DELITOS INFORMÁTICOS

Declaro estar informado de la investigación con fines académicos, y que mediante el presente cuestionario que tiene como objetivo determinar los niveles de percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022. Se recogerá la información pertinente, por lo que participo de manera voluntaria, honesta y anónima.

INSTRUCCIONES:

Marca con un aspa (x) la respuesta que mejor represente para usted el grado en el que se encuentra de acuerdo con las preguntas, siguiendo la escala valorativa del 1 al 5.

La siguiente tabla especifica el significado de la escala de valoración recién mencionada.

Nunca (N)	Casi nunca (CN)	A veces (AV)	Casi siempre (CS)	Siempre (S)
1	2	3	4	5

N°	Dimensiones / ítems	Valoraciones				
Variable 1: DELITOS INFORMÁTICOS						
D1	**Fraude informático**	**N**	**CN**	**AV**	**CS**	**S**
1	¿ ¿Ha sido víctima de hackeo de información a través de su tablet, dispositivo móvil o Pc?					
2	¿Ha tenido problemas de alteración de datos personales o confidenciales causados por fraude interno de su entidad bancaria?					
D2	**Estafa informática**	**N**	**CN**	**AV**	**CS**	**S**
3	¿Alguna vez ha recibido correos electrónicos falsos que simulan ser sitios web oficial de alguna entidad bancaria?					
4	¿Han logrado estafarlo bajo esta modalidad de delito por medio de su correo electrónico?					
5	¿Ha recibido usted mensajes de texto spam o falsos que se hacen pasar por un					

	representante de banco?					
6	¿Han logrado engañarlo con la modalidad anterior, obteniendo su información personal, o datos como contraseñas o número de cuentas?					
7	¿Usted ha recibido llamadas telefónicas desconocidas en el que intentan sacarle información, contraseñas u otros datos de sus tarjetas bancarias?					
8	¿Los delincuentes han logrado su objetivo y ha sido estafado por medio de llamada telefónica?					
D3	**Hurto informático**	**N**	**CN**	**AV**	**CS**	**S**
9	¿Usted ha sido víctima de robo de dinero de sus cuentas bancarias de manera sistemática?					
10	¿Alguna vez personas ajenas han realizado compras con el dinero disponible en sus tarjetas sin su consentimiento?					
11	¿Alguna vez se han apropiado de su título valor (título de propiedad, de auto, cheques, factura electrónica, etc.) de manera digital?					

FICHA TÉCNICA DE INSTRUMENTO

I.DATOS INFORMATIVOS:

1.1 **Técnica:** Encuesta

1.2 **Tipo de instrumento:** Cuestionario

1.3 **Lugar:** Ciudad de Chimbote

1.4 **Forma de aplicación:** Individual

1.5 **Autor:** Mantilla Barrón Carmen Thalía y Gonzales Ita Mirtha Daniela

1.6 **Medición:** Delitos Informáticos

1.7 **Tiempo de aplicación:** 15 minutos

II. OBJETIVO DEL INSTRUMENTO

Describir las modalidades de delitos informáticos recurrentes a los que se ven expuestos los usuarios en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022

III.VALIDACIÓN Y CONFIABILIDAD

El instrumento fue sometido a juicio de expertos, con la finalidad de poder analizar las proposiciones para comprobar si los ítems utilizados están bien definidos en relación al tema de investigación planteado, y si las instrucciones son claras y precisas, para evitar confusión al desarrollar la prueba. Para la validación se emplearon procedimientos, como: selección de los expertos en investigación y en la temática de estudio a quienes se les proporcionó la matriz de operacionalización de variables para que pueda ser evaluada permitiendo verificar si realmente los ítems cumplen con cada uno de los indicadores propuestos.

Para establecer la confiabilidad del instrumento, se aplicó una prueba piloto en 20 personas; posterior a ello, los resultados fueron sometidos a los procedimientos del método Alfa de Cronbach, el cual es un coeficiente estadístico y mide que tan confiable es el instrumento (Hernández y Mendoza, 2018).

Con ello se obtuvo que el cálculo de confiabilidad del instrumento fue $\alpha = 0{,}853$ resultado que a valoración e interpretación se asume como una confiabilidad muy buena, que permite determinar que el instrumento, proporciona la confiabilidad necesaria para su aplicación.

Estadísticas de fiabilidad	
Alfa de Cronbach	N° de elementos
,853	11

Nivel de confiabilidad Muy buena

IV. DIRIGIDO A:

383 usuarios de entidades bancarias, Chimbote.

V. MATERIALES NECESARIOS

Fotocopias del instrumento, lápiz, borrador.

VI. DESCRIPCIÓN DEL INSTRUMENTO

El instrumento de recolección de datos estuvo compuesto por 11 ítems con una valoración de escala de Likert de 1 a 5 puntos que fueron distribuidos en función a las dimensiones que conforman la variable “Delito Informático”.

La evaluación de los resultados se realizó por dimensiones calculando el promedio de los ítems que corresponden.

6.1. Opciones de respuestas

Nº de ítems	Opciones de respuestas	Puntuación
1;2;3;4;5;6;7;8;9;10;11	Siempre	5
	Casi siempre	4
	A veces	3
	Casi nunca	2
	Nunca	1

6.2. Distribución de ítems por dimensiones

DELITOS INFORMATICOS	**Fraude informático**	1,2
	Estafa informática	3,4,5,6,7,8
	Hurto informático	9,10,11

VI. NIVELES DE VALORIZACIÓN

PUNTAJE POR DIMENSIÓN Y VARIABLE

A nivel de variable				
	Total de ítems	**Puntaje**	**Escala**	**Valoración**
DELITOS INFORMATICOS	11	55	41 a 55	Alto
			27 a 40	Medio
			11 a 26	Bajo
A nivel de dimensiones de Percepción de seguridad				
Dimensión	**Total de ítems**	**Puntaje**	**Escala**	**Valoración**
Fraude informático	2	10	8 – 10	Alto
			6 - 7	Medio
			1 – 5	Bajo
Estafa informática	6	30	23 – 30	Alto
			15- 22	Medio
			6 – 14	Bajo
Hurto informático	3	15	12 – 15	Alto
			8 - 11	Medio
			3 – 7	Bajo

CUESTIONARIO PARA MEDIR LA VARIABLE PERCEPCION DE SEGURIDAD

Declaro estar informado de la investigación con fines académicos, y que mediante el presente cuestionario que tiene como objetivo determinar los niveles de percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2021. Se recogerá la información pertinente, por lo que participo de manera voluntaria, honesta y anónima.

INSTRUCCIONES:

Marca con un aspa (x) la respuesta que mejor represente para usted el grado en el que se encuentra de acuerdo con las preguntas, siguiendo la escala valorativa del 1 al 5.

La siguiente tabla especifica el significado de la escala de valoración recién mencionada.

Nunca (N)	Casi nunca (CN)	A veces (AV)	Casi siempre (CS)	Siempre (S)
1	2	3	4	5

N°	Dimensiones / ítems	Valoraciones				
Variable 2: PERCEPCIÓN DE SEGURIDAD						
D1	**Niveles de seguridad**	**N**	**CN**	**AV**	**CS**	**S**
12	¿Se siente usted seguro con la entidad bancaria en la que es usuario?					
13	¿Se siente usted seguro al utilizar la banca por Internet de la entidad financiera de la que usted es usuario?					
14	¿Cree usted que es poco probable que suceda un delito informático que atente en sus cuentas?					
15	¿Considera usted peligroso el utilizar las plataformas bancarias por el medio virtual?					
D2	**Sensaciones de seguridad**	**N**	**CN**	**AV**	**CS**	**S**
16	¿Confía usted en las plataformas digitales del banco al que es usuario?					
17	¿Realizar transacciones bancarias por internet					

	le causa inseguridad?					
18	¿Debido al incremento de delitos informáticos, ha considerado dejar de realizar transacciones bancarias por internet?					
D3	**Seguridad informática**	**N**	**CN**	**AV**	**CS**	**S**
19	Como cliente del banco, ¿recibe recomendaciones para prevenir ser víctima de fraudes o estafas en sus operaciones digitales?					
20	¿Conoce cómo responder ante un evento delictivo o fraude en sus cuentas bancarias?					
21	¿La entidad bancaria le ofrece información necesaria sobre las formas más seguras de realizar sus operaciones financieras?					
22	¿Conoce usted sus derechos como cliente de una entidad bancaria?					

FICHA TÉCNICA DE INSTRUMENTO

I. DATOS INFORMATIVOS:

1.8 **Técnica:** Encuesta

1.9 **Tipo de instrumento:** Cuestionario

1.10 **Lugar:** Ciudad de Chimbote

1.11 **Forma de aplicación:** Individual

1.12 **Autor:** Mantilla Barrón Carmen Thalía y Gonzales Ita Mirtha Daniela

1.13 **Medición:** Percepción de Seguridad

1.14 **Tiempo de aplicación:** 15 minutos

II. OBJETIVO DEL INSTRUMENTO

Describir los niveles de percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

III.VALIDACIÓN Y CONFIABILIDAD

El instrumento fue sometido a juicio de expertos, con la finalidad de poder analizar las proposiciones para comprobar si los ítems utilizados están bien definidos en relación al tema de investigación planteado, y si las instrucciones son claras y

precisas, para evitar confusión al desarrollar la prueba. Para la validación se emplearon procedimientos, como: selección de los expertos en investigación y en la temática de estudio a quienes se les proporcionó la matriz de operacionalización de variables para que pueda ser evaluada permitiendo verificar si realmente los ítems cumplen con cada uno de los indicadores propuestos.

Para establecer la confiabilidad del instrumento, se aplicó una prueba piloto en 20 personas; posterior a ello, los resultados fueron sometidos a los procedimientos del método Alfa de Cronbach, el cual es un coeficiente estadístico y mide que tan confiable es el instrumento (Hernández y Mendoza, 2018).

Con ello se obtuvo que el cálculo de confiabilidad del instrumento fue α= 0,846 resultado que a valoración e interpretación se asume como una confiabilidad muy buena, que permite determinar que el instrumento, proporciona la confiabilidad necesaria para su aplicación.

Estadísticas de fiabilidad	
Alfa de Cronbach	N° de elementos
,846	11

Nivel de confiabilidad Muy buena

IV. DIRIGIDO A:

383 usuarios de entidades bancarias, Chimbote.

V. MATERIALES NECESARIOS

Fotocopias del instrumento, lápiz, borrador.

VII. DESCRIPCIÓN DEL INSTRUMENTO

El instrumento de recolección de datos estuvo compuesto por 11 ítems con una valoración de escala de Likert de 1 a 5 puntos que fueron distribuidos en función a las dimensiones que conforman la variable “Percepción de Seguridad”.

La evaluación de los resultados se realizó por dimensiones calculando el promedio de los ítems que corresponden.

7.1. Opciones de respuestas

Nº de ítems	Opciones de respuestas	Puntuación
12,13,14,15,16,17,18,19,20,21,22	Siempre	5
	Casi siempre	4
	A veces	3
	Casi nunca	2
	Nunca	1

Para analizar los resultados de percepción de seguridad y sus dimensiones, se hizo uso de niveles de valoración, los cuales son: Bajo, Medio y Alto; según corresponda.

Niveles de valoración en la encuesta	Niveles de valoración para los resultados
Siempre	Alto
Casi siempre	
A veces	Medio
Casi nunca	Bajo
Nunca	

7.2. Distribución de ítems por dimensiones

PERCEPCION DE SEGURIDAD	**Niveles de seguridad**	12,13,14,15
	Sensaciones de seguridad	16,17,18
	Seguridad informática	19,20,21,22

VIII. NIVELES DE VALORIZACIÓN

PUNTAJE POR DIMENSIÓN Y VARIABLE

A nivel de variable				
PERCEPCION DE SEGURIDAD	**Total de ítems**	**Puntaje**	**Escala**	**Valoración**
	12	60	45 a 60	Alto

			29 a 44	Medio
			12 a 28	Bajo
A nivel de dimensiones de Percepción de seguridad				
Dimensión	**Total de ítems**	**Puntaje**	**Escala**	**Valoración**
Niveles de seguridad	4	25	16 – 20	Alto
			10 - 15	Medio
			4 – 9	Bajo
Sensaciones de seguridad	3	15	12 – 15	Alto
			8- 11	Medio
			3 – 7	Bajo
Seguridad informática	4	15	16 – 20	Alto
			10 - 15	Medio
			4 – 9	Bajo

Anexo 3. Calculo del tamaño de la muestra.

Fórmula finita para la determinación del tamaño de la muestra

$$n = \frac{\mathrm{N} * Z^2 * p * q}{e^2 * (N-1) + Z^2 * p * q}$$

Donde:

n= tamaño de la muestra

Z= Nivel de confianza

e= margen de error

p=variabilidad positiva

q=variabilidad negativa

N= tamaño de población

$$n = \frac{214198 * 1.96^2 * 0.50 * 0.50}{0.05^2 * (214198-1) + 1.96^2 * 0.50 * 0.50}$$

n= 383

Anexo 4. Confiabilidad de los instrumentos de recolección de datos

Confiabilidad del instrumento de Delitos informáticos

RESULTADO DEL ANÁLISIS DE CONFIABILIDAD DEL INSTRUMENTO PARA MEDIR LA VARIABLE: DELITOS INFORMATICOS

Estadísticas de fiabilidad	
Alfa de Cronbach	N° de elementos
,853	11

Nivel de confiabilidad Muy buena

Estadísticas de total de elemento				
	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
1.- ¿Ha sido víctima de hackeo de su sistema de información en su Tablet, PC u otro ordenador?	20,25	49,566	,313	,855
2.- ¿Ha tenido problemas de alteración de datos personales o confidenciales causados por fraude interno de su entidad bancaria?	20,10	51,989	,132	,865
3.- ¿Alguna vez ha recibido correos electrónicos falsos que simulan ser sitios web oficial de alguna entidad bancaria?	18,15	45,397	,546	,840
4.- ¿Han logrado estafarlo bajo esta modalidad de delito por medio de su correo electrónico?	20,30	46,747	,423	,850
5.- ¿Ha recibido usted mensajes de texto spam o falsos que se hacen pasar por un representante de banco?	17,75	47,882	,438	,847

6.- ¿Han logrado engañarlo con la modalidad anterior, obteniendo su información personal, o datos como contraseñas o número de cuentas?	20,00	39,474	,764	,819
7.- ¿Usted ha recibido llamadas telefónicas desconocidas en el que intentan sacarle información, contraseñas u otros datos de sus tarjetas bancarias?	18,75	48,092	,264	,866
8.- ¿Los delincuentes han logrado su objetivo y ha sido estafado por medio de llamada telefónica?	20,30	46,116	,676	,833
9.- ¿Usted ha sido víctima de robo de dinero de sus cuentas bancarias de manera sistemática?	20,30	41,695	,807	,818
10.- ¿Alguna vez personas ajenas han realizado compras con el dinero disponible en sus tarjetas sin su consentimiento?	20,30	41,695	,807	,818
11.- ¿Alguna vez se han apropiado de su título valor (título de propiedad, de auto, etc.) de manera sistemática?	20,30	41,695	,807	,818

Confiabilidad del instrumento de Percepción de Seguridad

RESULTADO DEL ANÁLISIS DE CONFIABILIDAD DEL INSTRUMENTO PARA MEDIR LA VARIABLE: PERCEPCION DE SEGURIDAD

Estadísticas de fiabilidad	
Alfa de Cronbach	N° de elementos
,846	11

Nivel de confiabilidad Muy buena

Estadísticas de total de elemento				
	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
12.- ¿Se siente usted seguro con la entidad bancaria en la que es usuario?	30,25	47,355	,403	,843
13.- ¿Se siente usted seguro al utilizar la banca por Internet de la entidad financiera de la que usted es usuario?	30,60	45,832	,460	,839
14.- ¿Cree usted que es poco probable que suceda un delito informático que atente en sus cuentas?	30,20	50,168	,211	,856
15.- ¿Considera usted peligroso el utilizar las plataformas bancarias por el medio virtual?	30,35	46,976	,485	,837
16.- ¿Confía usted en las plataformas digitales del banco al que es usuario?	30,55	46,787	,493	,836
17.- ¿Realizar transacciones bancarias por internet le causa inseguridad?	30,30	44,747	,617	,827
18.- ¿Debido al incremento de delitos informáticos, ha considerado dejar de realizar transacciones bancarias por internet?	30,50	48,158	,397	,843
19.- Como cliente del banco, ¿recibe recomendaciones para prevenir ser víctima de fraudes o estafas en sus operaciones digitales?	30,65	42,871	,701	,819
20.- ¿Conoce cómo responder ante un evento delictivo o fraude en sus cuentas bancarias?	30,50	43,947	,512	,836

21.- ¿La entidad bancaria le ofrece información necesaria sobre las formas más seguras de realizar sus operaciones financieras?	30,50	40,474	,720	,815
22.- ¿La entidad bancaria le brinda a usted información sobre las características de los canales de atención con los que cuenta?	30,60	41,621	,816	,809

Base de Datos de Prueba Piloto

1	NUNCA
2	CASI NUNCA
3	A VECES
4	CASI SIEMPRE
5	SIEMPRE

VALORACION DE LA RESPUESTA				
N	CN	AV	CS	S
1	2	3	4	5

		VARIABLE DELITOS INFORMATICOS											VARIABLE PERCEPCION DE SEGURIDAD										
	Encuestados	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22
	1	1	1	3	1	4	1	3	1	1	1	1	3	3	3	3	3	4	4	3	2	5	3
	2	4	1	3	1	3	1	3	2	1	1	1	3	3	3	3	3	3	3	3	3	3	3
	3	1	1	3	1	3	1	3	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3
	4	1	1	3	1	3	1	3	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3
	5	1	2	2	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	6	1	4	3	1	4	2	3	1	1	1	1	4	3	3	4	3	4	3	4	2	3	3
	7	1	2	4	4	4	4	3	4	4	4	4	3	3	3	3	3	2	3	2	3	2	2
	8	1	2	2	1	3	1	1	2	1	1	1	1	1	5	5	1	5	2	2	5	1	2
	9	1	1	3	1	4	1	1	1	1	1	1	3	3	3	2	3	3	4	5	4	3	3
	10	3	3	5	1	5	1	5	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3
	11	2	1	5	1	5	1	5	1	1	1	1	4	4	4	3	4	2	2	1	2	1	1
	12	1	2	3	1	4	1	3	1	1	1	1	4	1	5	2	4	2	2	2	2	2	2
	13	1	1	4	1	4	1	2	1	1	1	1	4	4	3	3	3	3	5	2	3	3	3
	14	1	1	3	1	5	1	5	1	1	1	1	5	4	3	3	4	3	2	3	5	5	3
	15	1	1	5	5	5	5	4	1	1	1	1	3	1	4	4	2	4	4	2	1	2	2
	16	1	2	2	1	4	1	1	1	1	1	1	4	4	4	3	3	3	3	3	2	4	4
	17	1	1	5	1	3	1	3	1	1	1	1	3	3	5	5	5	5	3	5	5	5	5
	18	3	2	5	1	5	5	3	3	5	5	5	3	3	3	3	3	3	3	3	3	3	3
	19	1	1	3	1	5	1	3	1	1	1	1	5	5	2	4	2	4	4	3	3	3	4
	20	1	1	4	1	3	1	3	1	1	1	1	3	3	3	3	3	4	3	4	5	5	5

Anexo 5. Validez de los instrumentos de recolección de datos

Hernández, et ál. (2014) sostienen que la validación consta de una serie de rangos mediante el cual un instrumento es medido, cada rango tiene una valoración que va desde el más bajo hasta el más alto, y se puede definir como inaceptable hasta excelente respectivamente. Esta medición se realiza para cada variable y la confiabilidad del instrumento se encargará de medir el nivel de confianza para cada uno de los ítems que conforma el instrumento de recolección de datos.

En esta investigación la validación pasó por la evaluación de tres expertos especialistas en administración quienes a su criterio dieron la aprobación de cada una de las preguntas que conformaban el cuestionario.

Para la medición de la fiabilidad se utilizó el coeficiente Alfa de Cronbach, midiéndose cada uno de los ítems y variables y saber que tan confiable es el instrumento.

Intervalo Alfa de Cronbach	Valoración de fiabilidad de los ítems
[0,00 a 0,50[	Inaceptable
[0,50 a 0,60[	Pobre
[0,60 a 0,70[	Débil
[0,70 a 0,80[	Aceptable
[0,80 a 0,90[	Bueno
[0,90 a 1,00]	Excelente

Delitos Informáticos y Percepción de Seguridad de los clientes en las operaciones en línea de los Sistemas Bancarios, Chimbote-2021

Variable 1: Delitos informáticos

Variable	Dimensión	Indicador	Definición de indicador	Ítems	Opción de respuesta					Criterios de evaluación								Observación y/o recomendaciones
										Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítem		Relación entre el ítem y la opción de respuesta		
										si	no	si	no	si	no	si	no	
Variable 1: Delitos informáticos Objetivo: Describir las modalidades de delitos informáticos recurrentes a los que se ven expuestos los usuarios y entes bancarios peruanos de Chimbote.	FRAUDE INFORMÁTICO	FRAUDE AL SISTEMA	El sujeto burla las medidas de seguridad de los sistemas informáticos y accede al patrimonio virtual de la víctima.	¿Ha sido víctima de hackeo a través de su tablet, dispositivo móvil o PC?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
		FRAUDE EN LOS DATOS	El delincuente altera los datos en los sistemas informáticos para obtener algún beneficio propio.	¿Ha tenido problemas de alteración de datos personales o confidenciales causados por fraude interno de su entidad bancaria?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
	ESTAFA INFORMÁTICA	PHISHING	Modalidad de estafa por medio de **correo electrónico** en la que se apropian de información personal de clientes y sus cuentas bancarias.	¿Alguna vez ha recibido correos electrónicos falsos que simulan ser sitios web oficial de alguna entidad bancaria?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
				¿Han logrado estafarlo bajo esta modalidad de delito por medio de su correo electrónico?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
		SMISHING	Modalidad de estafa por **mensajes de texto** en la que se apropian de información personal de clientes y sus cuentas bancarias.	¿Ha recibido usted mensajes de texto spam o falsos que se hacen pasar por un representante de banco?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
				¿Han logrado engañarlo con la modalidad anterior, obteniendo su información personal, o datos como contraseñas o número de cuentas?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
		VISHING	Modalidad de estafa por medio de **llamadas telefónicas** en la que el	¿Usted ha recibido llamadas telefónicas desconocidas en el	Nunca (1)	Casi nunca	A veces	Casi siempre	Siempre (5)	X		X		X		X		

			usuario accede a otorgar información personal o confidencial.	que intentan sacarle información, contraseñas u otros datos de sus tarjetas bancarias?		(2)	(3)	(4)											
				¿Los delincuentes han logrado su objetivo y ha sido estafado por medio de llamada telefónica?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X			
	HURTO INFORMÁTICO	HURTO SISTEMÁTICO	Robo del patrimonio en el que el delincuente retira **dinero o ahorros** de las cuentas bancarias de otra persona.	¿Usted ha sido víctima de robo de dinero de sus cuentas bancarias de manera sistemática?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X			
				¿Alguna vez, personas ajenas han realizado compras con el dinero disponible en sus tarjetas sin su consentimiento?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X			
		HURTO DE VALORES	Hurto de bienes como títulos de valores, programas, etc.	¿Alguna vez se han apropiado de su título valor (título de propiedad, de auto, etc.) de manera digital?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X			

Variable 2: Percepción de seguridad

Variable	Dimensión	Indicador	Definición de indicador	Ítems	Opción de respuesta					Criterios de evaluación								Observación y/o recomendaciones
										Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítem		Relación entre el ítem y la opción de respuesta		
										si	no	si	no	si	no	si	no	
Variable 2: Percepción de Seguridad Objetivo: Identificar la **percepción de inseguridad** de usuarios víctimas de delitos informáticos de los sistemas bancarios de Chimbote.	NIVELES DE SEGURIDAD	SEGURO	Condición de ciertos mecanismos que aseguran estar libre de todo daño, amenaza peligro o riesgo	¿Se siente usted seguro con la entidad bancaria en la que es usuario?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	**X**		X		X		X		
				¿Se siente usted seguro al utilizar la banca por Internet de la entidad financiera de la que usted es usuario?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	**X**		X		X		X		
		DUDOSO	Es poco probable de que suceda un acontecimiento o hecho.	¿Cree usted que es poco probable que suceda un delito informático que atente en sus cuentas?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
		PELIGROSO		¿Considera usted peligroso el utilizar las plataformas bancarias por el medio virtual?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
	SENSACIONES DE SEGURIDAD	CONFIANZA	Es la esperanza o seguridad que tiene un individuo en alguien o en algo	¿Confía usted en las plataformas digitales del banco al que es usuario?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
		INCERTIDUMBRE	situación de desconocimiento o imposibilidad de medir o calcular los sucesos que ocasionan daños	¿Realizar transacciones bancarias por internet le causa inseguridad?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
		AMENAZA	Estado, evento, suceso o acontecimiento origen de riesgos que no se pueden medir ni calcular	¿Debido al incremento de delitos informáticos, ha considerado dejar de realizar transacciones bancarias por internet?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
	SEGURIDAD INFORMÁTICA	PREVENCIÓN DE RIESGOS		Como cliente del banco, ¿recibe recomendaciones para prevenir ser víctima de fraudes o estafas en sus operaciones digitales?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
		POLITICAS	Pautas para marcar los límites a los que deben producirse las acciones.	¿Conoce cómo responder ante un evento delictivo o fraude en sus cuentas bancarias?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		

		ASPECTOS NORMATIVOS	Conjunto de normas o reglas aplicadas a una determinada actividad o asunto con el fin de establecer su funcionamiento.	¿La entidad bancaria le ofrece información necesaria sobre las formas más seguras de realizar sus operaciones financieras?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		
				¿Conoce usted sus derechos como cliente de una entidad bancaria?	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)	X		X		X		X		

Experto 1: Validación de delitos Informáticos y Percepción de Seguridad

RESULTADO DE LA VALIDACIÓN DEL INSTRUMENTO

NOMBRE DEL INSTRUMENTO: Cuestionario delitos informáticos y percepción de seguridad

OBJETIVO: Describir los niveles de percepción de seguridad de los clientes en las operaciones en línea de los sistemas bancarios de Chimbote, periodo 2022.

DIRIGIDO A: Usuarios la banca digital de entidades bancarias de Chimbote

VALORACIÓN DEL INSTRUMENTO:

Deficiente	Regular	Bueno	Muy Bueno	Excelente
		X		

APELLIDOS Y NOMBRES DEL EVALUADOR: INCACUTIPA CCALLO LIDIA

GRADO ACADÉMICO DEL EVALUADOR: LICENCIADA EN ADMINISTRACIÓN DE EMPRESAS

Lic. Lidia Incacutipa Ccallo
DNI: 44449555

Nota: Quien valide el instrumento debe asignarle una valoración marcando con un aspa en el casillero que corresponda

REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Aplicativo Guía

Resultado

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
INCACUTIPA CCALLO, LIDIA **DNI 44449555**	BACHILLER EN ADMINISTRACION **Fecha de diploma: 14/05/2014** **Modalidad de estudios:** - **Fecha matrícula: Sin información (***)** **Fecha egreso: Sin información (***)**	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***
INCACUTIPA CCALLO, LIDIA **DNI 44449555**	LICENCIADA EN ADMINISTRACION - Fecha de diploma: 04/07/2014 Modalidad de estudios: -	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***

(***) Ante la falta de información, puede presentar su consulta formalmente a través de la mesa de partes virtual en el siguiente enlace https://enlinea.sunedu.gob.pe/

Experto 2: Validación de delitos informáticos y percepción de seguridad

RESULTADO DE LA VALIDACIÓN DEL INSTRUMENTO

NOMBRE DEL INSTRUMENTO: Cuestionario delitos informáticos y percepción de seguridad

OBJETIVO: Describir los niveles de percepción de seguridad de los clientes en las operaciones en línea del sistema bancario en Chimbote, periodo 2022.

DIRIGIDO A: Usuarios de la banca digital de las entidades bancarias de Chimbote

VALORACIÓN DEL INSTRUMENTO:

Deficiente	Regular	Bueno	Muy Bueno	Excelente
		X		

APELLIDOS Y NOMBRES DEL EVALUADOR: Huamán Paz Angie Vanessa

GRADO ACADÉMICO DEL EVALUADOR: Licenciada en Administración de Empresas

Lic. Huamán Paz Angie Vanessa
DNI: 72156872

Nota: Quien valide el instrumento debe asignarle una valoración marcando con un aspa en el casillero que corresponda.

Resultado

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
HUAMAN PAZ, ANGIE VANESSA **DNI 72156872**	**BACHILLER EN ADMINISTRACION** **Fecha de diploma: 13/09/16** **Modalidad de estudios: PRESENCIAL** **Fecha matrícula: 03/03/2011** **Fecha egreso: 16/07/2016**	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***
HUAMAN PAZ, ANGIE VANESSA **DNI 72156872**	**LICENCIADA EN ADMINISTRACION** **Fecha de diploma: 28/02/17** **Modalidad de estudios: PRESENCIAL**	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***

Experto 3: Validación de delitos informáticos y percepción de seguridad

RESULTADO DE LA VALIDACIÓN DEL INSTRUMENTO

NOMBRE DEL INSTRUMENTO: Cuestionario delitos informáticos y percepción de seguridad

OBJETIVO: Describir los niveles de percepción de seguridad de los clientes en las operaciones en línea del sistema bancario en Chimbote, periodo 2022.

DIRIGIDO A: Usuarios de la banca digital de las entidades bancarias de Chimbote

VALORACIÓN DEL INSTRUMENTO:

Deficiente	Regular	Bueno	Muy Bueno	Excelente
		X		

APELLIDOS Y NOMBRES DEL EVALUADOR: Huamán Paz Angie Vanessa

GRADO ACADÉMICO DEL EVALUADOR: Licenciada en Administración de Empresas

MBA. Varillas Uriel Edwin Adolfo
DNI: 09937724

Nota: Quien valide el instrumento debe asignarle una valoración marcando con un aspa en el casillero que corresponda.

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
VARILLAS URIOL, EDWIN ADOLFO **DNI 09937724**	**LICENCIADO EN ADMINISTRACION** **Fecha de diploma: 28/12/2005** **Modalidad de estudios: -**	UNIVERSIDAD PRIVADA SAN PEDRO ***PERU***
VARILLAS URIOL, EDWIN ADOLFO **DNI 09937724**	**BACHILLER EN CIENCIAS CONTABLES Y ADMINISTRATIVAS** **Fecha de diploma: 20/11/2003** **Modalidad de estudios: -** **Fecha matrícula: Sin información (***)** **Fecha egreso: Sin información (***)**	UNIVERSIDAD PRIVADA SAN PEDRO ***PERU***
VARILLAS URIOL, EDWIN ADOLFO **DNI 09937724**	**MAESTRO EN GESTION PUBLICA** **Fecha de diploma: 05/11/19** **Modalidad de estudios: PRESENCIAL** **Fecha matrícula: 20/08/2018** **Fecha egreso: 20/07/2019**	UNIVERSIDAD SAN PEDRO ***PERU***

Anexo 6. Tablas y figuras como resultado de la aplicación del instrumento.

Tabla 8.

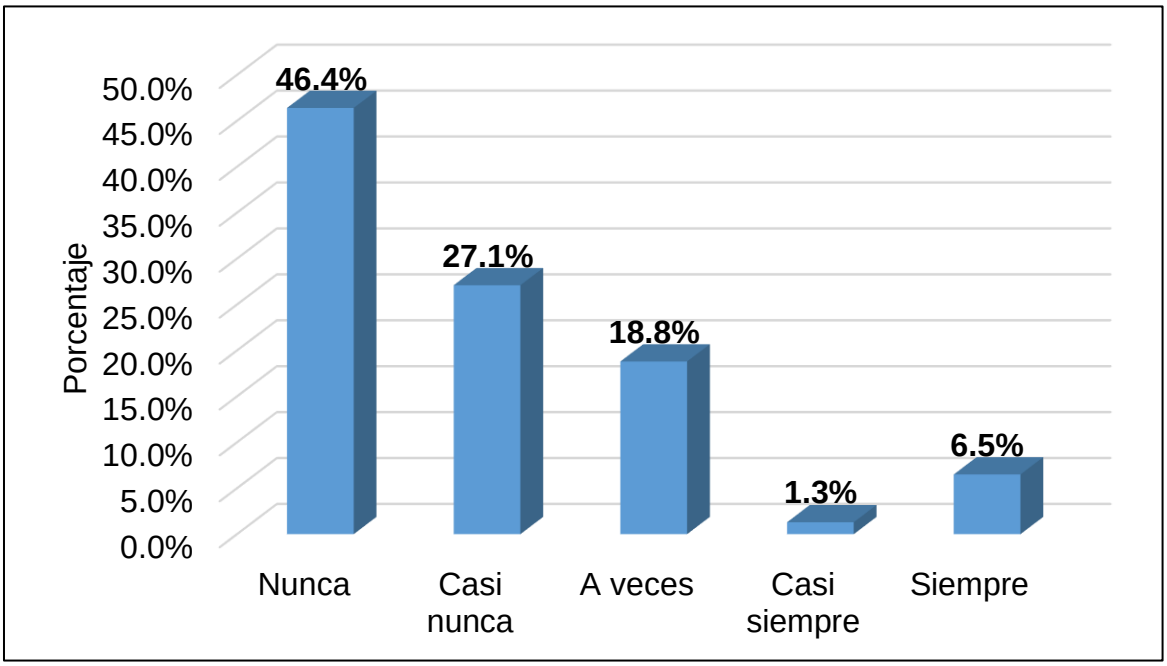
Pregunta formulada para medir la dimensión fraude informático: ¿Ha sido víctima de hackeo de su sistema de información en su Tablet, PC u otro ordenador?

	Frecuencia	Porcentaje
Nunca	178	46.4%
Casi nunca	104	27.1%
A veces	72	18.8%
Casi siempre	5	1.3%
Siempre	25	6.5%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 8.

Figura de barras de la pregunta formulada para medir la dimensión fraude informático: ¿Ha sido víctima de hackeo de su sistema de información en su Tablet, PC u otro ordenador?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 9.

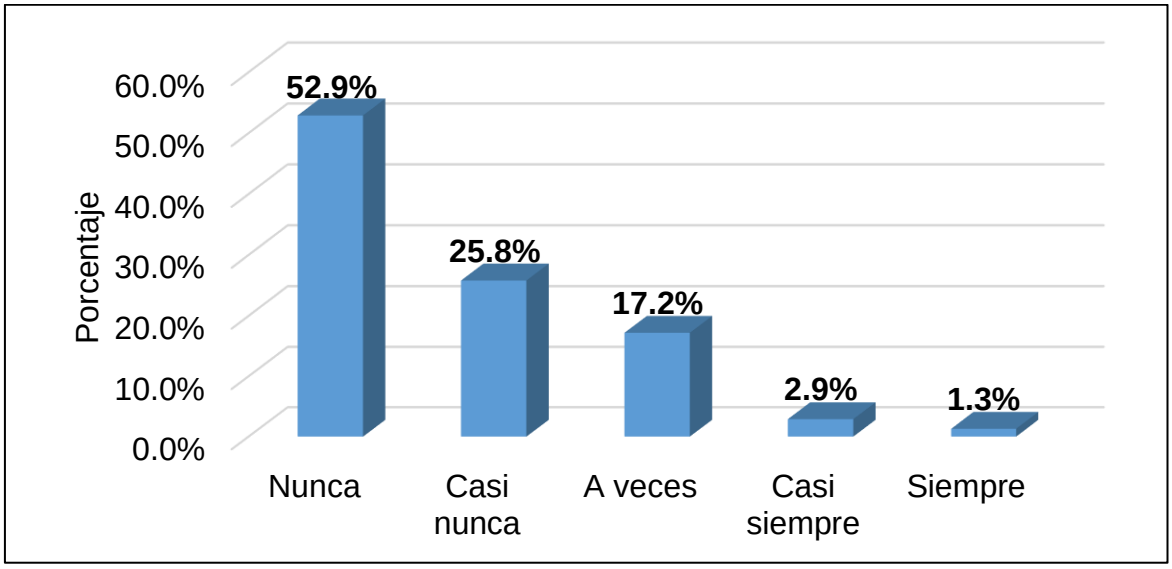
Pregunta formulada para medir la dimensión fraude informático: ¿Ha tenido problemas de alteración de datos personales o confidenciales causados por fraude interno de su entidad bancaria?

	Frecuencia	Porcentaje
Nunca	203	52.9%
Casi nunca	99	25.8%
A veces	66	17.2%
Casi siempre	11	2.9%
Siempre	5	1.3%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 9.

Figura de barras de la pregunta formulada para medir la dimensión fraude informático: ¿Ha tenido problemas de alteración de datos personales o confidenciales causados por fraude interno de su entidad bancaria?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 10.

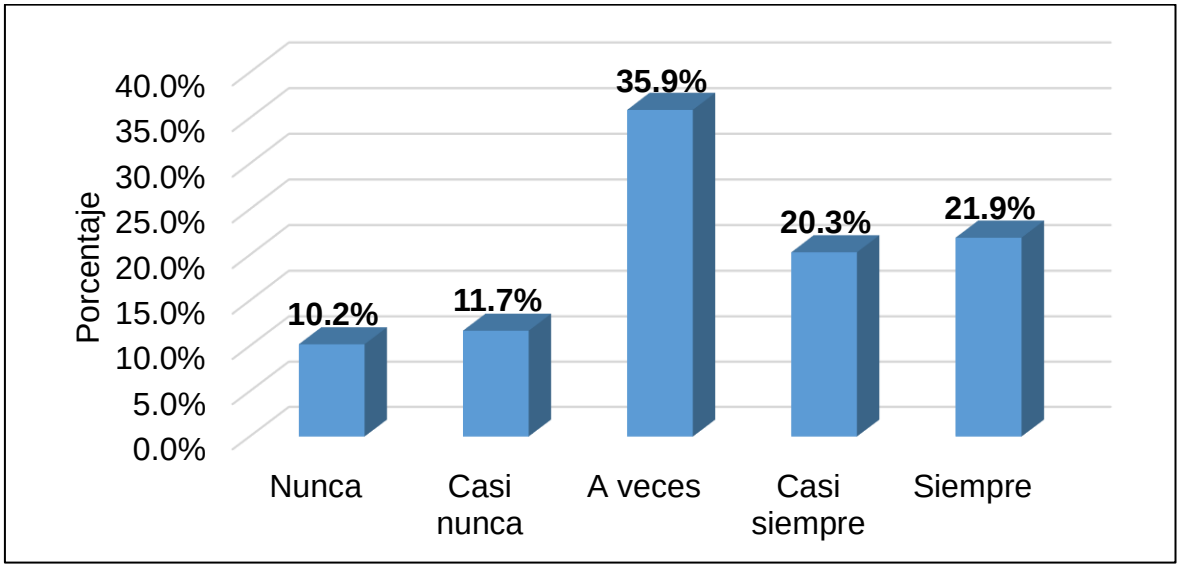
Pregunta formulada para medir la dimensión estafa informática: ¿Alguna vez ha recibido correos electrónicos falsos que simulan ser sitios web oficial de alguna entidad bancaria?

	Frecuencia	Porcentaje
Nunca	39	10.2%
Casi nunca	45	11.7%
A veces	138	35.9%
Casi siempre	78	20.3%
Siempre	84	21.9%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 10.

Figura de barras de la pregunta formulada para medir la dimensión estafa informática: ¿Alguna vez ha recibido correos electrónicos falsos que simulan ser sitios web oficial de alguna entidad bancaria?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 11.

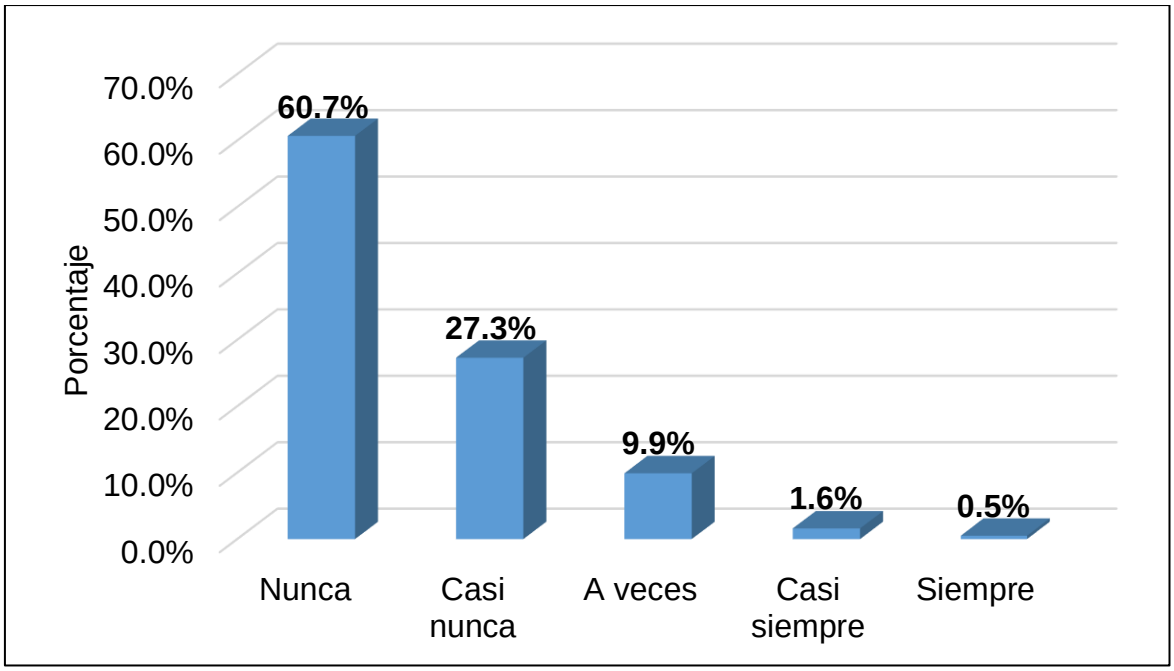
Pregunta formulada para medir la dimensión estafa informática: ¿Han logrado estafarlo bajo esta modalidad de delito por medio de su correo electrónico?

	Frecuencia	Porcentaje
Nunca	233	60.7%
Casi nunca	105	27.3%
A veces	38	9.9%
Casi siempre	6	1.6%
Siempre	2	0.5%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 11.

Figura de barras de la pregunta formulada para medir la dimensión estafa informática: ¿Han logrado estafarlo bajo esta modalidad de delito por medio de su correo electrónico?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 12.

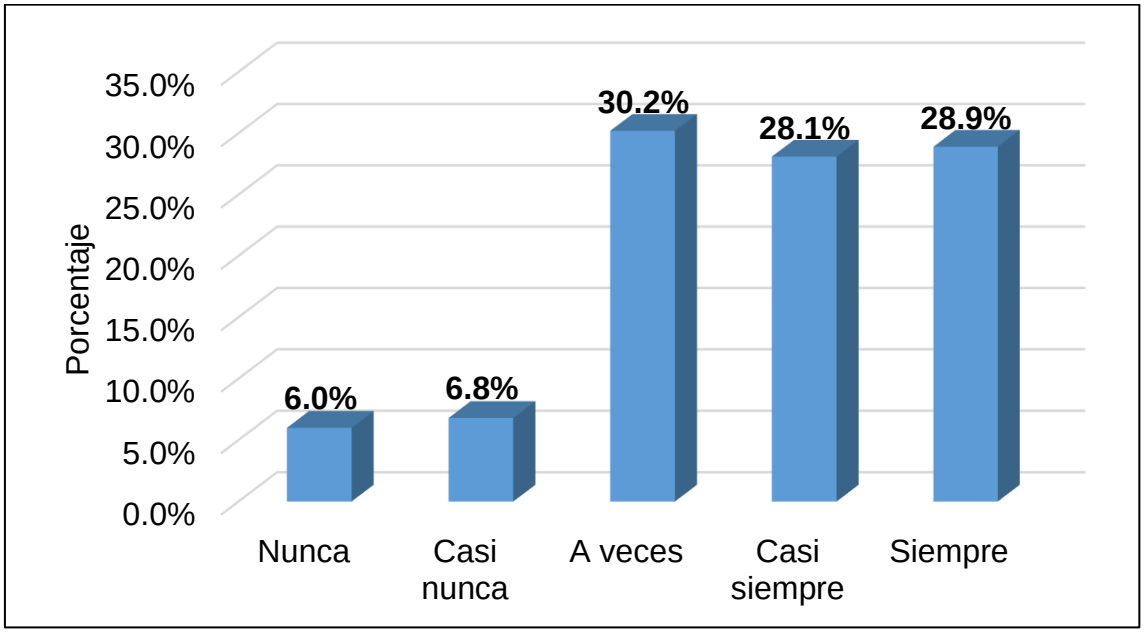
Pregunta formulada para medir la dimensión estafa informática: ¿Ha recibido usted mensajes de texto spam o falsos que se hacen pasar por un representante de banco?

	Frecuencia	Porcentaje
Nunca	23	6.0%
Casi nunca	26	6.8%
A veces	116	30.2%
Casi siempre	108	28.1%
Siempre	111	28.9%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 12.

Figura de barras de la pregunta formulada para medir la dimensión estafa informática: ¿Ha recibido usted mensajes de texto spam o falsos que se hacen pasar por un representante de banco?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 13.

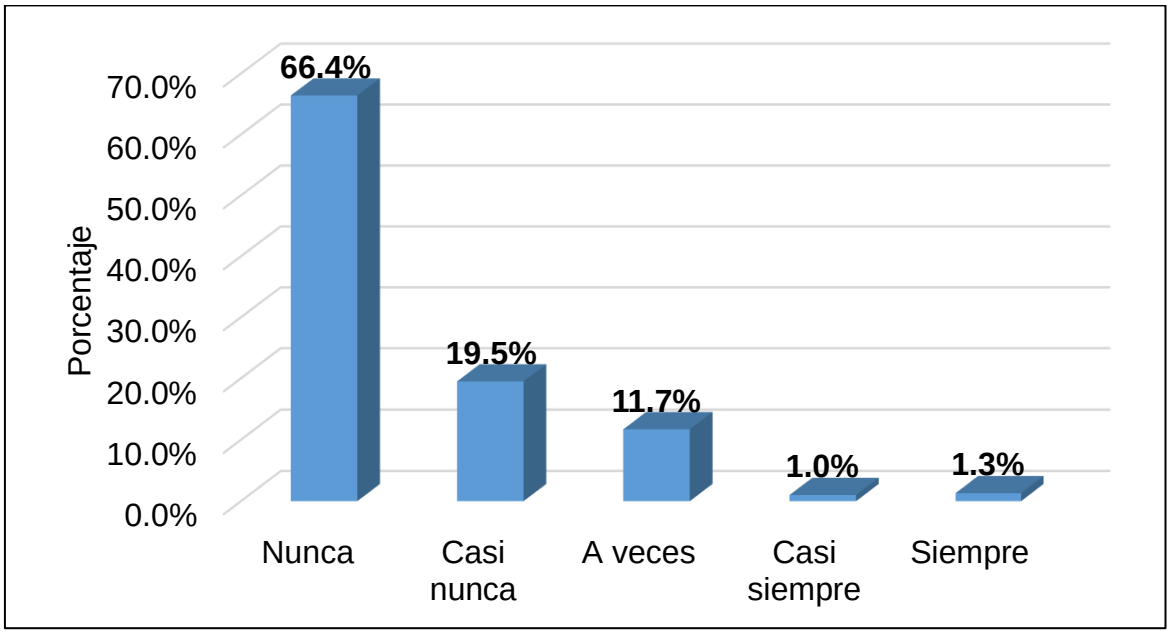
Pregunta formulada para medir la dimensión estafa informática: ¿Han logrado engañarlo con la modalidad anterior, obteniendo su información personal, o datos como contraseñas o número de cuentas?

	Frecuencia	Porcentaje
Nunca	225	66.4%
Casi nunca	75	19.5%
A veces	45	11.7%
Casi siempre	4	1.0%
Siempre	5	1.3%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 13.

Figura de barras de la pregunta formulada para medir la dimensión estafa informática: ¿Han logrado engañarlo con la modalidad anterior, obteniendo su información personal, o datos como contraseñas o número de cuentas?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 14.

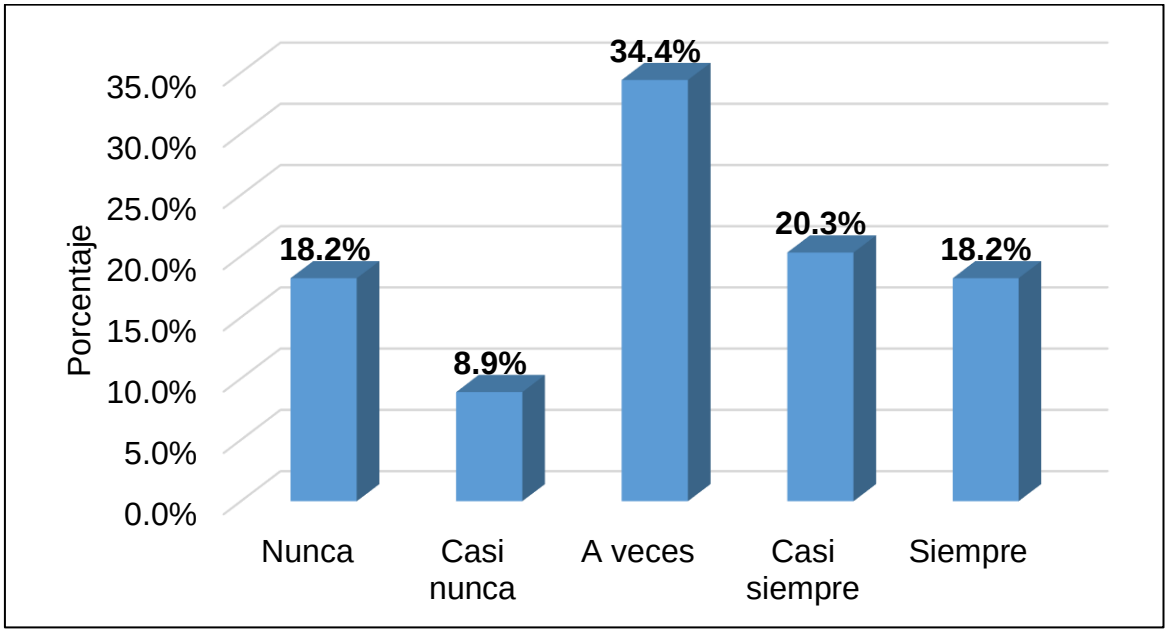
Pregunta formulada para medir la dimensión estafa informática: ¿Usted ha recibido llamadas telefónicas desconocidas en el que intentan sacarle información, contraseñas u otros datos de sus tarjetas bancarias?

	Frecuencia	Porcentaje
Nunca	70	18.2%
Casi nunca	34	8.9%
A veces	132	34.4%
Casi siempre	78	20.3%
Siempre	70	18.2%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 14.

Figura de barras de la pregunta formulada para medir la dimensión estafa informática: ¿Usted ha recibido llamadas telefónicas desconocidas en el que intentan sacarle información, contraseñas u otros datos de sus tarjetas bancarias?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 15.

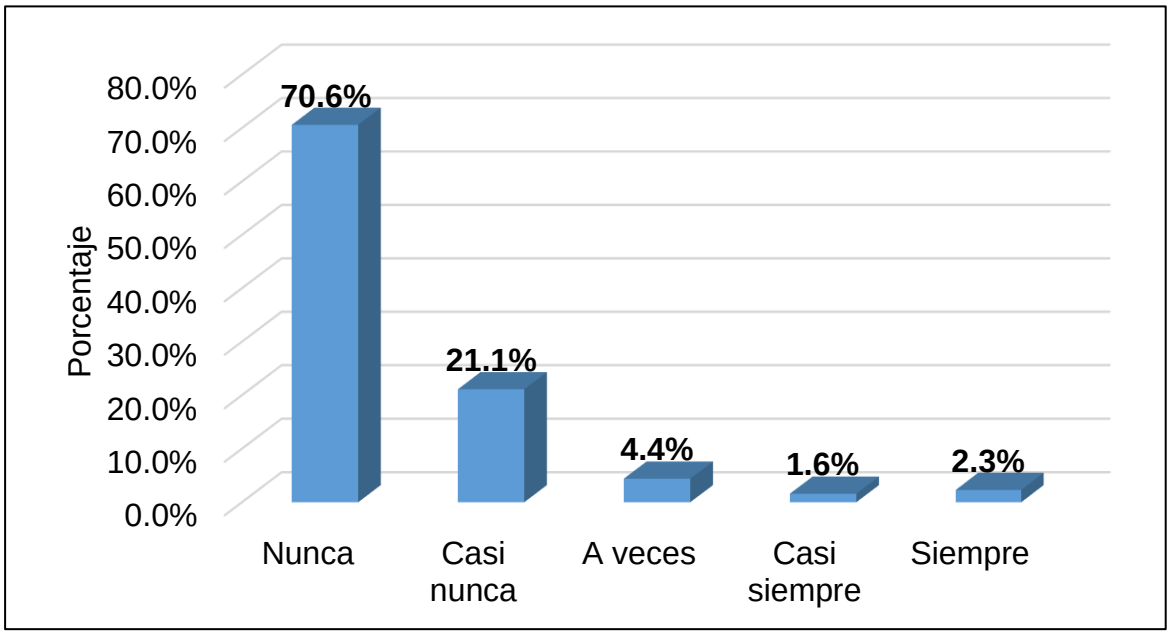
Pregunta formulada para medir la dimensión estafa informática: ¿Los delincuentes han logrado su objetivo y ha sido estafado por medio de llamada telefónica?

	Frecuencia	Porcentaje
Nunca	271	70.6%
Casi nunca	81	21.1%
A veces	17	4.4%
Casi siempre	6	1.6%
Siempre	9	2.3%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 15.

Figura de barras de la pregunta formulada para medir la dimensión estafa informática: ¿Los delincuentes han logrado su objetivo y ha sido estafado por medio de llamada telefónica?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 16.

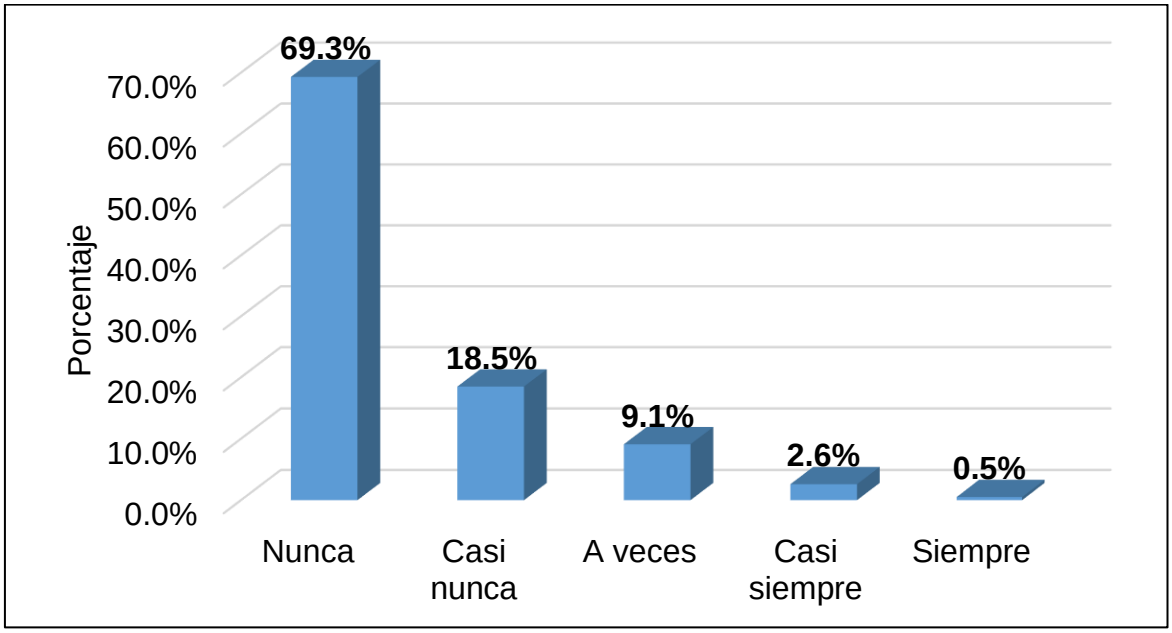
Pregunta formulada para medir la dimensión hurto informático: ¿Usted ha sido víctima de robo de dinero de sus cuentas bancarias de manera sistemática?

	Frecuencia	Porcentaje
Nunca	266	69.3%
Casi nunca	71	18.5%
A veces	35	9.1%
Casi siempre	10	2.6%
Siempre	2	0.5%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 16.

Figura de barras de la pregunta formulada para medir la dimensión hurto informático: ¿Usted ha sido víctima de robo de dinero de sus cuentas bancarias de manera sistemática?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 17.

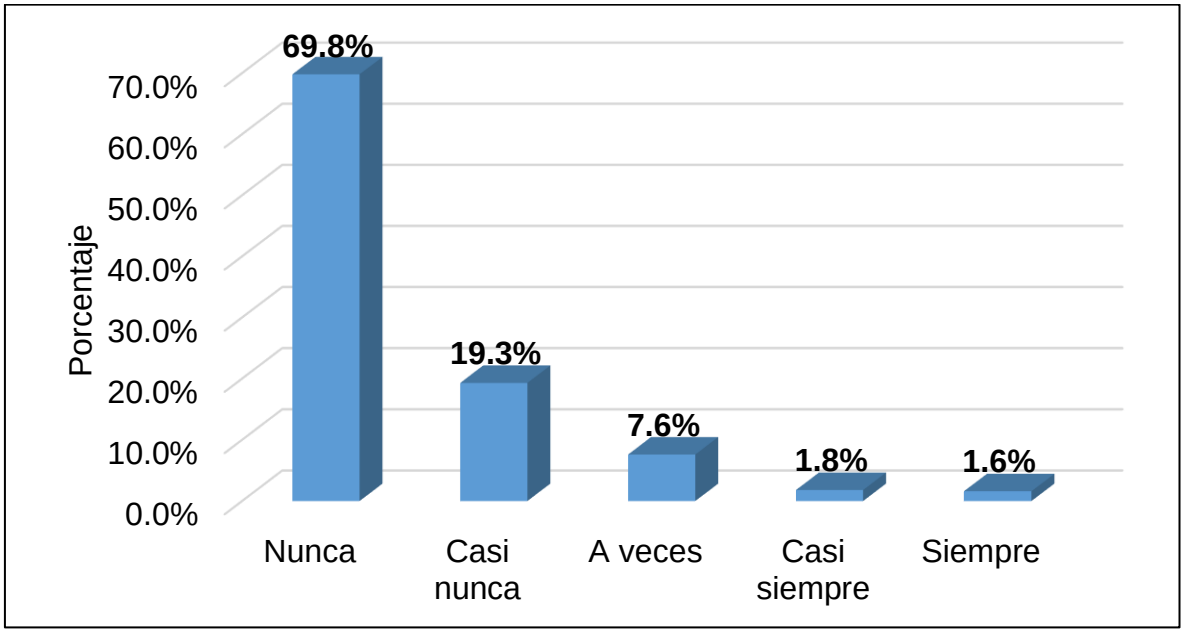
Pregunta formulada para medir la dimensión hurto informático: ¿Alguna vez personas ajenas han realizado compras con el dinero disponible en sus tarjetas sin su consentimiento?

	Frecuencia	Porcentaje
Nunca	268	69.8%
Casi nunca	74	19.3%
A veces	29	7.6%
Casi siempre	7	1.8%
Siempre	6	1.6%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 17.

Figura de barras de la pregunta formulada para medir la dimensión hurto informático: ¿Alguna vez personas ajenas han realizado compras con el dinero disponible en sus tarjetas sin su consentimiento?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 18.

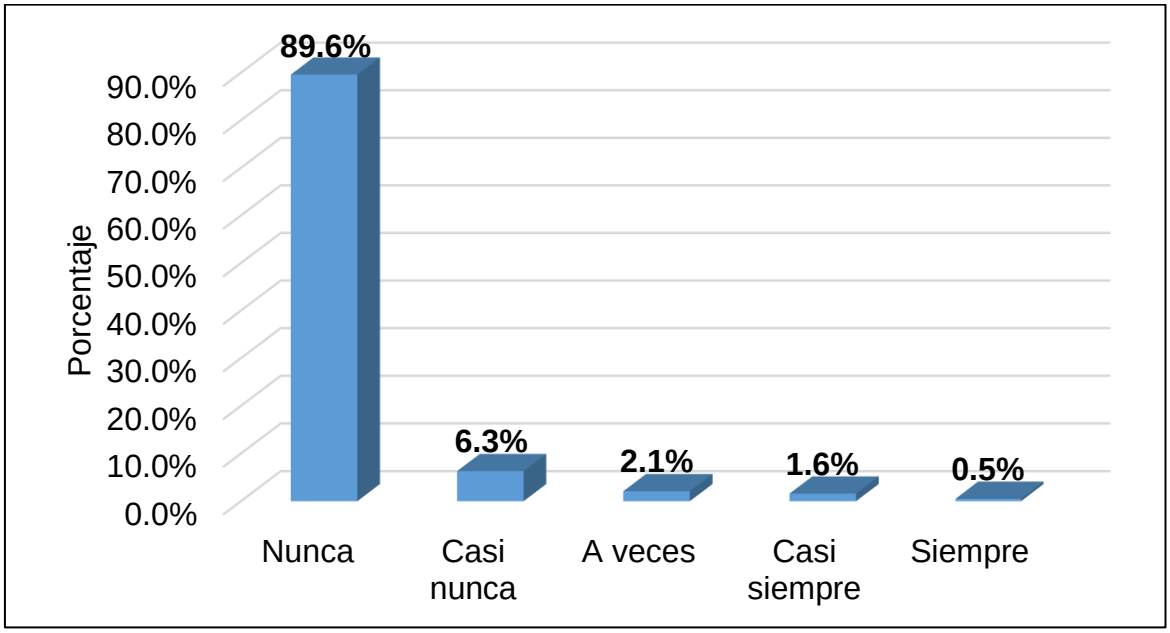
Pregunta formulada para medir la dimensión hurto informático: ¿Alguna vez se han apropiado de su título valor (título de propiedad, de auto, etc.) de manera sistemática?

	Frecuencia	Porcentaje
Nunca	334	89.6%
Casi nunca	24	6.3%
A veces	8	2.1%
Casi siempre	6	1.6%
Siempre	2	0.5%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 18.

Figura de barras para la pregunta formulada para medir la dimensión hurto informático: ¿Alguna vez se han apropiado de su título valor (título de propiedad, de auto, etc.) de manera sistemática?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 19.

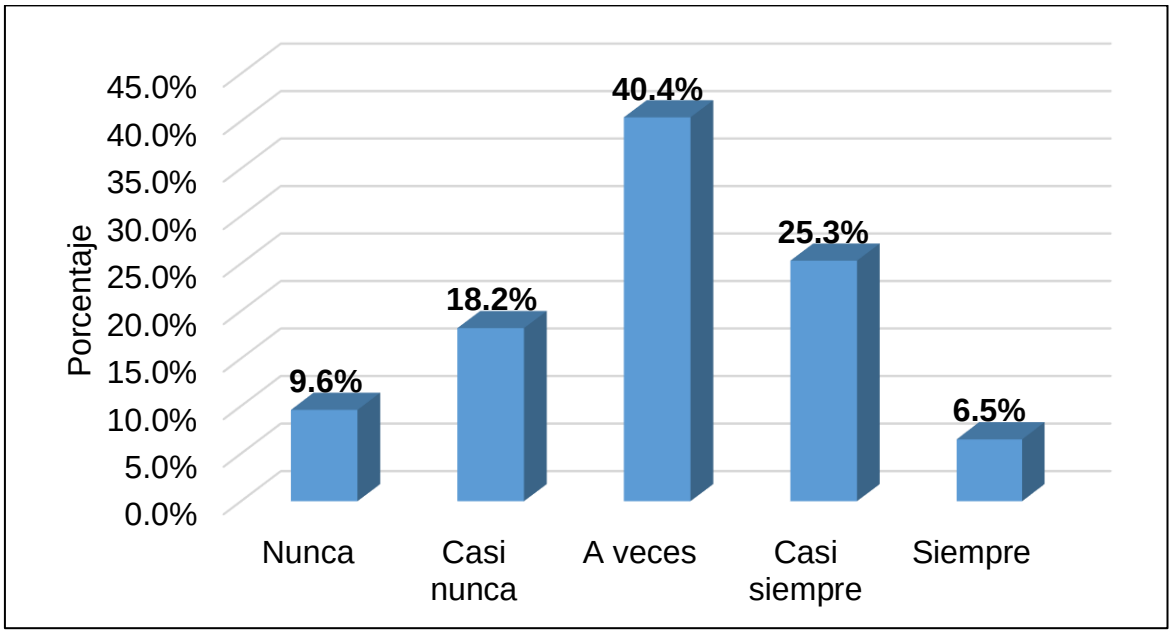
Pregunta formulada para medir la dimensión niveles de seguridad: ¿Se siente usted seguro con la entidad bancaria en la que es usuario?

	Frecuencia	Porcentaje
Nunca	37	9.6%
Casi nunca	70	18.2%
A veces	155	40.4%
Casi siempre	97	25.3%
Siempre	25	6.5%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 19.

Figura de barras de la pregunta formulada para medir la dimensión niveles de seguridad: ¿Se siente usted seguro con la entidad bancaria en la que es usuario?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 20.

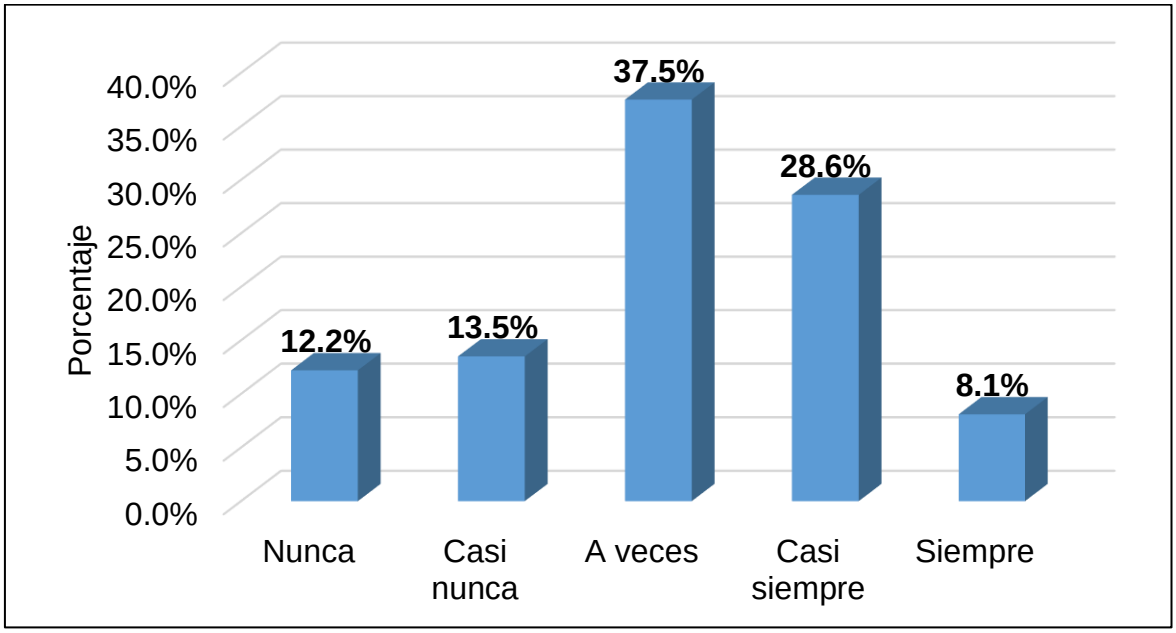
Pregunta formulada para medir la dimensión niveles de seguridad: ¿Se siente usted seguro al utilizar la banca por Internet de la entidad financiera de la que usted es usuario?

	Frecuencia	Porcentaje
Nunca	47	12.2%
Casi nunca	52	13.5%
A veces	144	37.5%
Casi siempre	110	28.6%
Siempre	31	8.1%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 20.

Figura de barras de la pregunta formulada para medir la dimensión niveles de seguridad: ¿Se siente usted seguro al utilizar la banca por Internet de la entidad financiera de la que usted es usuario?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 21.

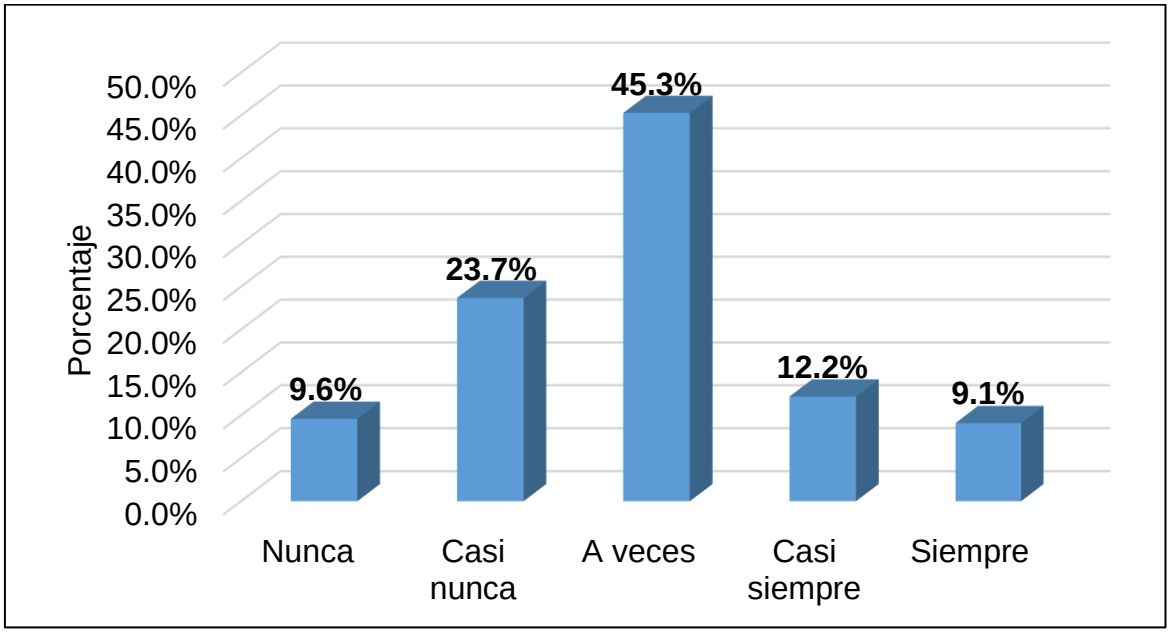
Pregunta formulada para medir la dimensión niveles de seguridad: ¿Cree usted que es poco probable que suceda un delito informático que atente en sus cuentas?

	Frecuencia	Porcentaje
Nunca	37	9.6%
Casi nunca	91	23.7%
A veces	174	45.3%
Casi siempre	47	12.2%
Siempre	35	9.1%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 21.

Figura de barras de la pregunta formulada para medir la dimensión niveles de seguridad: ¿Cree usted que es poco probable que suceda un delito informático que atente en sus cuentas?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 22.

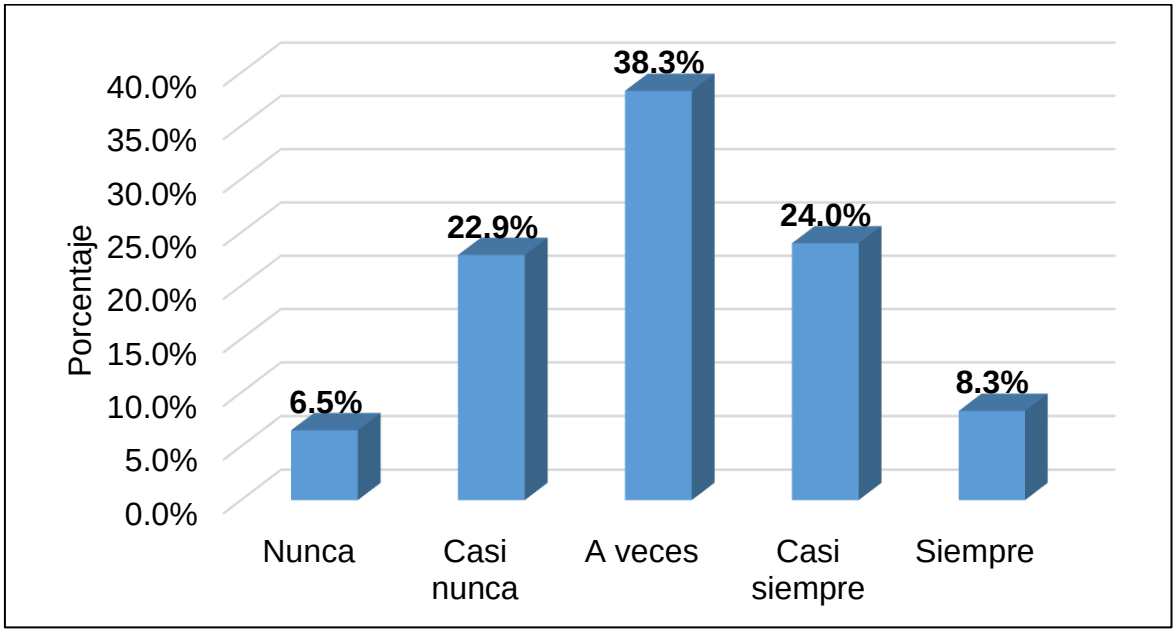
Pregunta formulada para medir la dimensión niveles de seguridad: ¿Considera usted peligroso el utilizar las plataformas bancarias por el medio virtual?

	Frecuencia	Porcentaje
Nunca	25	6.5%
Casi nunca	88	22.9%
A veces	147	38.3%
Casi siempre	92	24.0%
Siempre	32	8.3%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 22.

Figura de barras de la pregunta formulada para medir la dimensión niveles de seguridad: ¿Considera usted peligroso el utilizar las plataformas bancarias por el medio virtual?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 23.

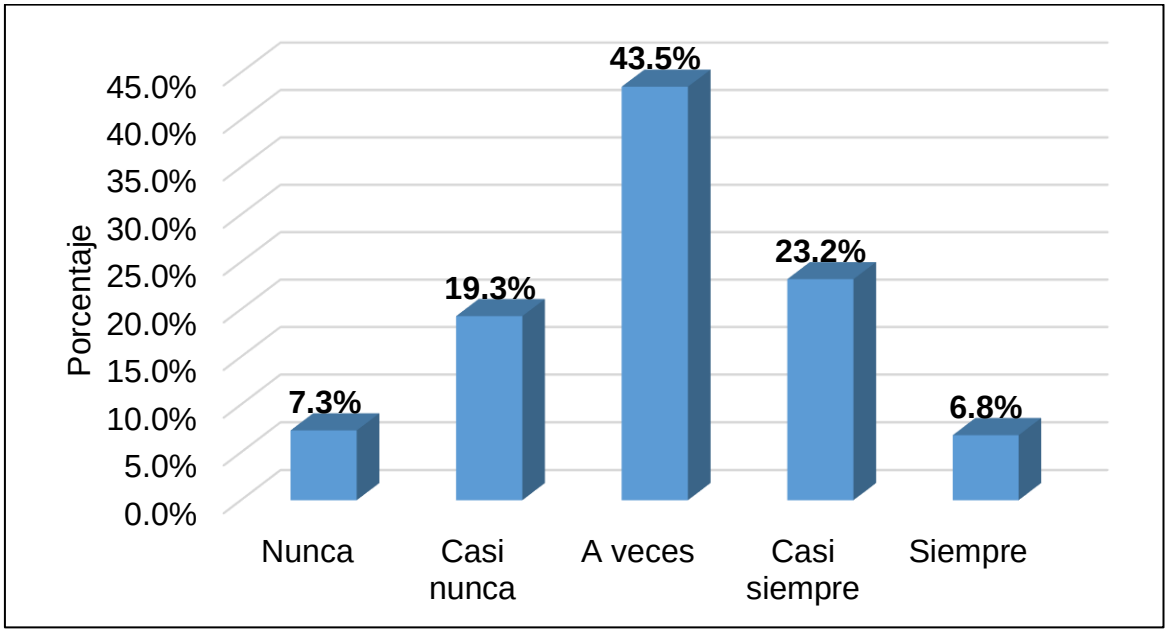
Pregunta formulada para medir la dimensión sensaciones de seguridad: ¿Confía usted en las plataformas digitales del banco al que es usuario?

	Frecuencia	Porcentaje
Nunca	28	7.3%
Casi nunca	74	19.3%
A veces	167	43.5%
Casi siempre	89	23.2%
Siempre	26	6.8%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 23.

Figura de barras de la pregunta formulada para medir la dimensión sensaciones de seguridad: ¿Confía usted en las plataformas digitales del banco al que es usuario?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 24.

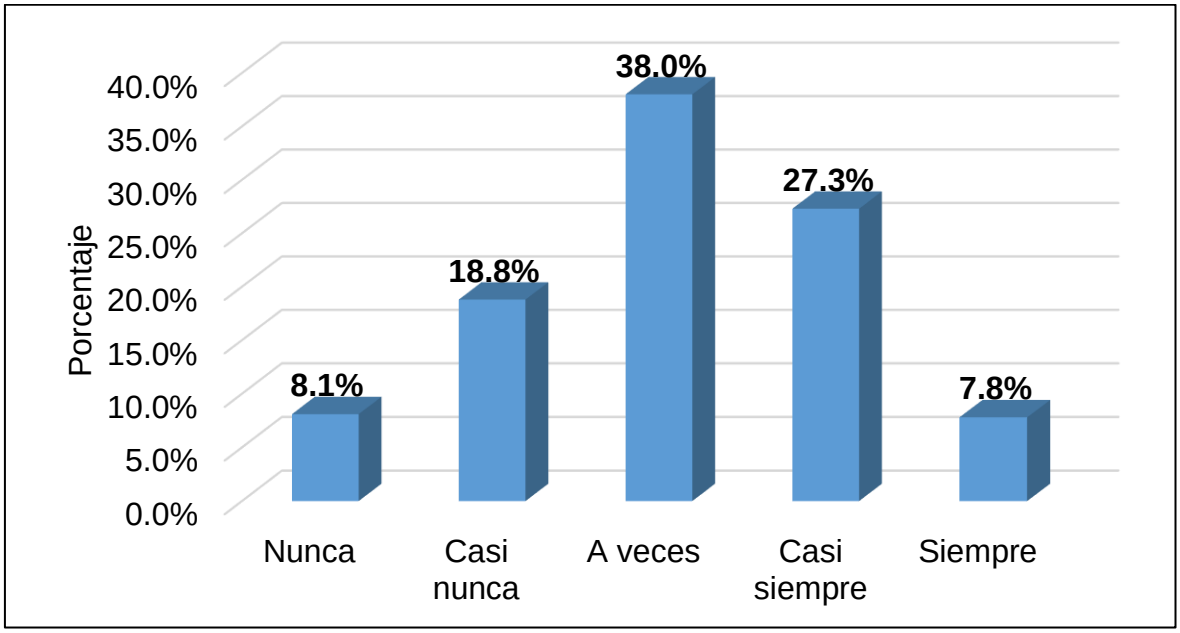
Pregunta formulada para medir la dimensión sensaciones de seguridad: ¿Realizar transacciones bancarias por internet le causa inseguridad?

	Frecuencia	Porcentaje
Nunca	31	8.1%
Casi nunca	72	18.8%
A veces	146	38.0%
Casi siempre	105	27.3%
Siempre	30	7.8%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 24.

Figura de barras de la pregunta formulada para medir la dimensión sensaciones de seguridad: ¿Realizar transacciones bancarias por internet le causa inseguridad?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 25.

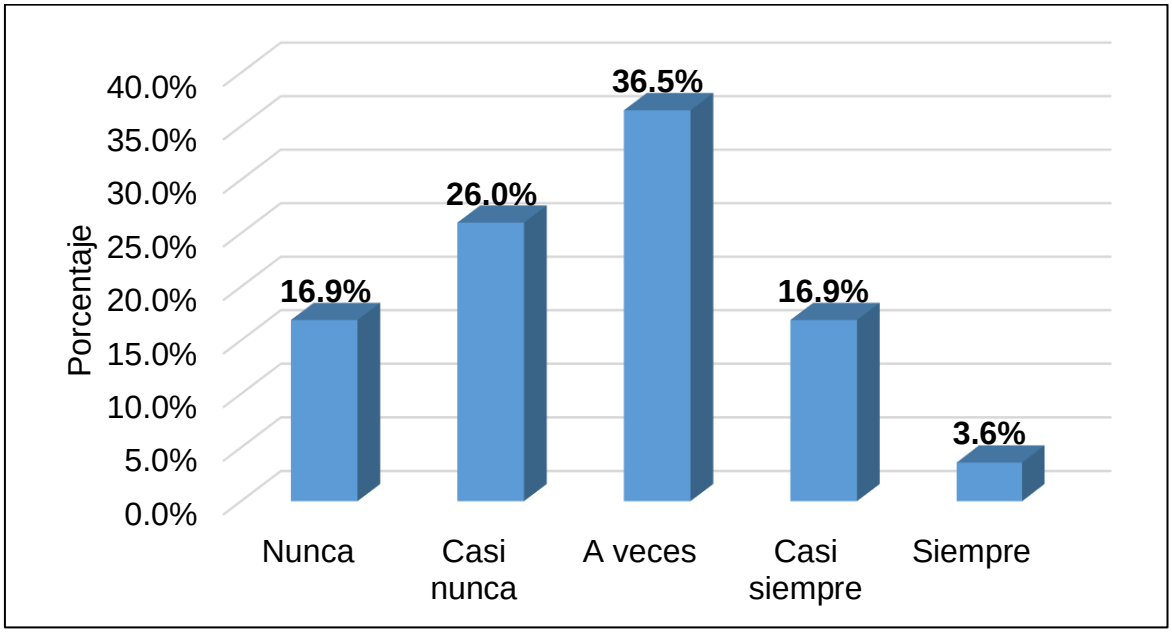
Pregunta formulada para medir la dimensión sensaciones de seguridad: ¿Debido al incremento de delitos informáticos, ha considerado dejar de realizar transacciones bancarias por internet?

	Frecuencia	Porcentaje
Nunca	65	16.9%
Casi nunca	100	26.0%
A veces	140	36.5%
Casi siempre	65	16.9%
Siempre	14	3.6%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 25.

Figura de barras de la pregunta formulada para medir la dimensión sensaciones de seguridad: ¿Debido al incremento de delitos informáticos, ha considerado dejar de realizar transacciones bancarias por internet?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 26.

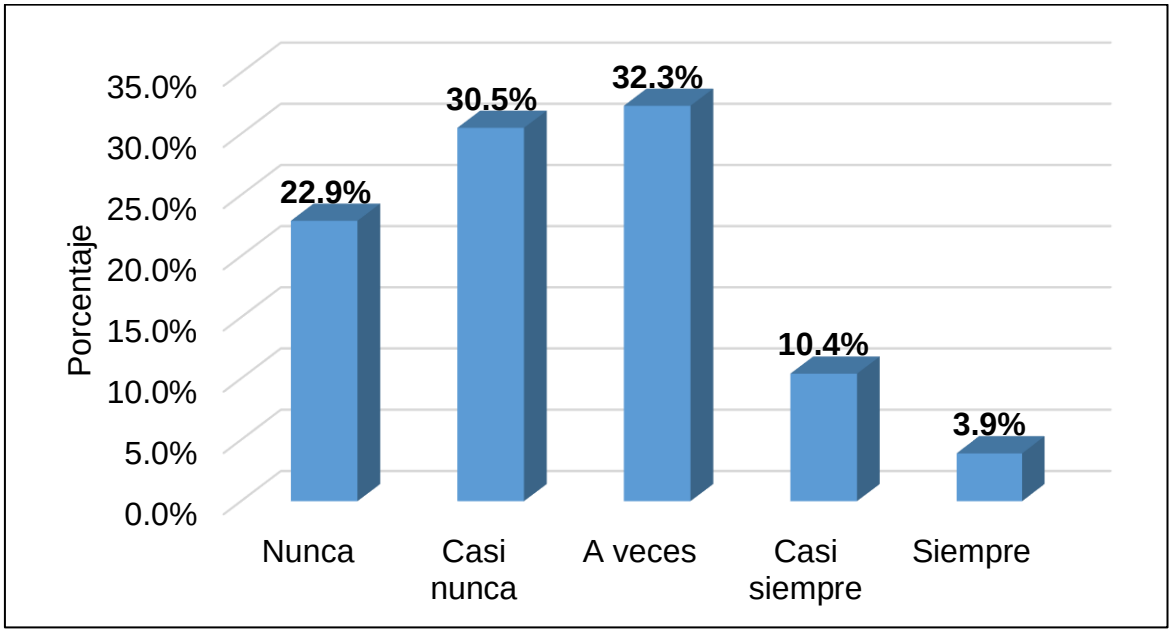
Pregunta formulada para medir la dimensión seguridad informática: Como cliente del banco, ¿recibe recomendaciones para prevenir ser víctima de fraudes o estafas en sus operaciones digitales?

	Frecuencia	Porcentaje
Nunca	88	22.9%
Casi nunca	117	30.5%
A veces	124	32.3%
Casi siempre	40	10.4%
Siempre	15	3.9%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 26.

Figura de barras de la pregunta formulada para medir la dimensión seguridad informática: Como cliente del banco, ¿recibe recomendaciones para prevenir ser víctima de fraudes o estafas en sus operaciones digitales?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 27.

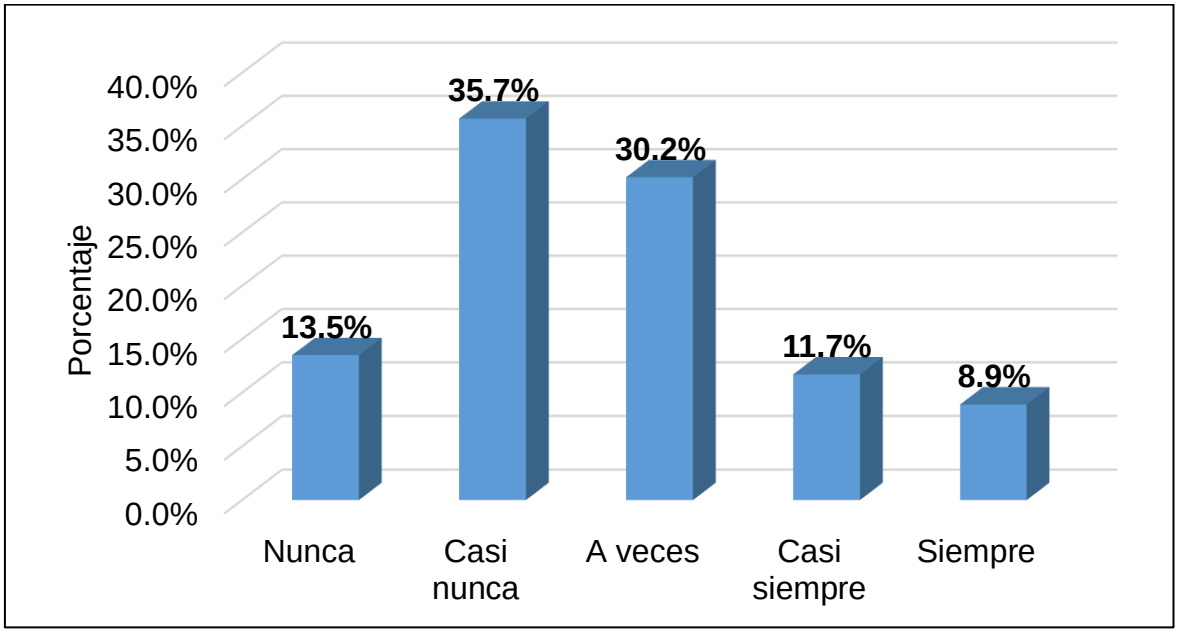
Pregunta formulada para medir la dimensión seguridad informática: ¿Conoce cómo responder ante un evento delictivo o fraude en sus cuentas bancarias?

	Frecuencia	Porcentaje
Nunca	52	13.5%
Casi nunca	137	35.7%
A veces	116	30.2%
Casi siempre	45	11.7%
Siempre	34	8.9%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 27.

Figura de barras de la pregunta formulada para medir la dimensión seguridad informática: ¿Conoce cómo responder ante un evento delictivo o fraude en sus cuentas bancarias?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 28.

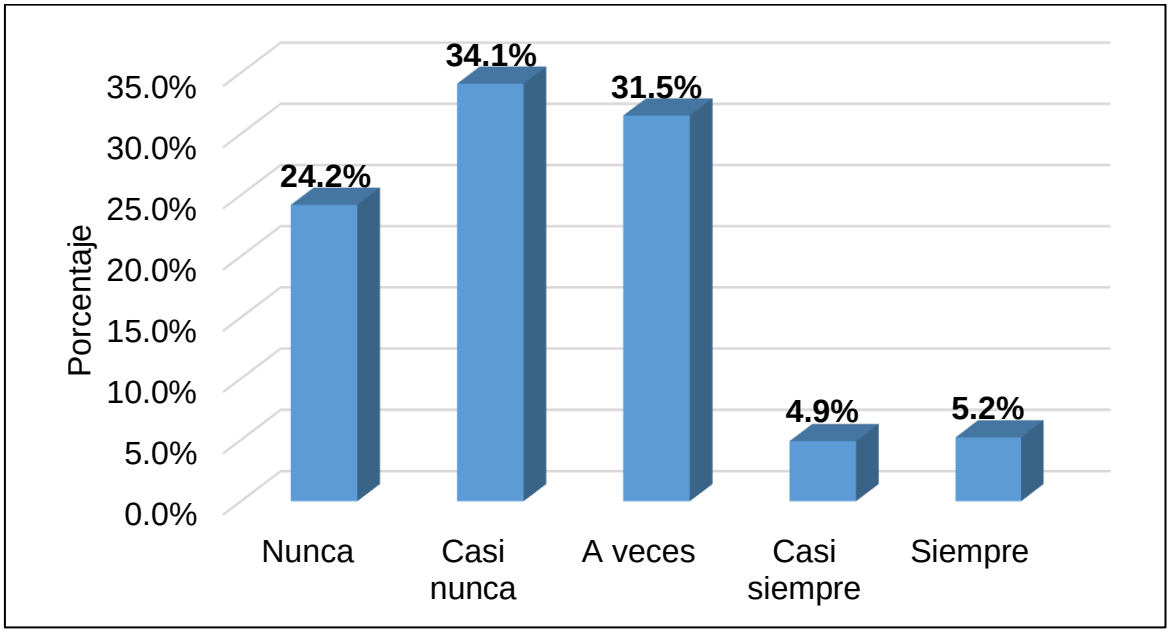
Pregunta formulada para medir la dimensión seguridad informática: ¿La entidad bancaria le ofrece información necesaria sobre las formas más seguras de realizar sus operaciones financieras?

	Frecuencia	Porcentaje
Nunca	93	24.2%
Casi nunca	131	34.1%
A veces	121	31.5%
Casi siempre	19	4.9%
Siempre	20	5.2%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 28.

Figura de barras de la pregunta formulada para medir la dimensión seguridad informática: ¿La entidad bancaria le ofrece información necesaria sobre las formas más seguras de realizar sus operaciones financieras?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Tabla 29.

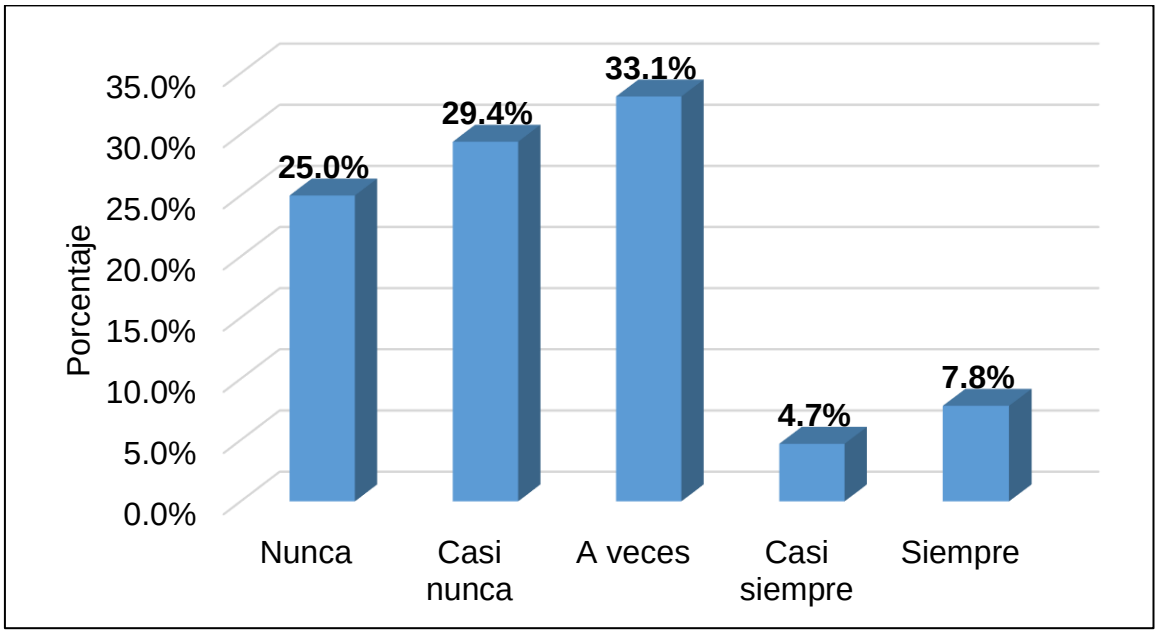
Pregunta formulada para medir la dimensión seguridad informática: ¿Conoce usted sus derechos como cliente de una entidad bancaria?

	Frecuencia	Porcentaje
Nunca	96	25.0%
Casi nunca	113	29.4%
A veces	127	33.1%
Casi siempre	18	4.7%
Siempre	30	7.8%
Total	384	100%

Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

Figura 29.

Figura de barras de la pregunta formulada para medir la dimensión seguridad informática: ¿Conoce usted sus derechos como cliente de una entidad bancaria?



Nota. Esta tabla muestra datos estadísticos reunidos de la encuesta realizada a los usuarios en línea de entidades bancarias de Chimbote.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE CIENCIAS EMPRESARIALES

ESCUELA PROFESIONAL DE ADMINISTRACIÓN

Declaratoria de Autenticidad de los Asesores

Nosotros, ESPINOZA DE LA CRUZ MANUEL ANTONIO, SALAZAR LLANOS JUAN FRANCISCO docentes de la FACULTAD DE CIENCIAS EMPRESARIALES de la escuela profesional de ADMINISTRACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - CHIMBOTE, asesores de Tesis titulada: "Delitos Informáticos y percepción de seguridad de los clientes en las operaciones en línea de los Sistemas Bancarios, Chimbote-2022", cuyos autores son GONZALES ITA MIRTHA DANIELA, MANTILLA BARRON CARMEN THALIA, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

Hemos revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

CHIMBOTE, 03 de Julio del 2022

Apellidos y Nombres del Asesor:	**Firma**
ESPINOZA DE LA CRUZ MANUEL ANTONIO **DNI:** 18195946 **ORCID:** 0000-0001-6290-4484	Firmado electrónicamente por: MANTONIOED el 03-07-2022 09:50:03
SALAZAR LLANOS JUAN FRANCISCO **DNI:** 44137812 **ORCID:** 0000-0001-8314-2634	Firmado electrónicamente por: SLLANOSJF el 05-07-2022 21:09:59

Código documento Trilce: TRI - 0318429

INVESTIGA UCV